Chapter 6

Towards classification

Introduction

In this chapter we introduce two group-theoretic notions that are pivotal tools in classification results of the kind that we want to achieve. We also use these tools to obtain some initial results about the structure of cyclic groups and of finite abelian groups with certain special orders.

The first notion is a construction called *direct product*, which produces a new group from two (or more) given ones. In some cases, the newly constructed group shares some of the properties of its ancestors, such as being abelian or being cyclic. Under certain conditions, it is possible to decompose a given group as the direct product of two or more of its subgroups. This is often useful because knowledge of the (smaller) subgroups may give important information about the larger product group. We explore these concepts in Section 1.

In Section 2 we use direct products to describe the structure of finite cyclic groups. More specifically, we explain when a finite cyclic group can be written as a direct product of cyclic groups of smaller order. We also show that there is only one cyclic group of a given order, up to isomorphism.

Our preoccupation with cyclic groups is because they are the simplest examples of abelian groups, and it is finite abelian groups that we will eventually classify.

The second notion we introduce is one that you might have encountered in your previous studies: that of a group *acting on a set*. In Section 3 we remind you about group actions and the Orbit–Stabiliser Theorem, and we give a range of examples. Then we use group actions to prove two important results about finite groups.

One is *Cayley's Theorem*, which tells us that any finite group can be viewed as a subgroup of a suitable symmetric group S_n.

The other is *Cauchy's Theorem*, a partial converse to Lagrange's Theorem that tells us that a finite group of order n has an element of order p for each prime divisor p of n. Cauchy's Theorem is proved by considering a particular action of a group on tuples of its elements.

Finally, we obtain some results about expressing a finite group as a direct product of subgroups in the special cases of abelian groups whose order is either a product of prime numbers or the power of a prime.

One of our main goals in this book is to classify finite abelian groups. We will not be ready to fully prove this by the end of this chapter, but we will have made considerable progress in this direction.

Chapter guide

Sections 1 and 2 require roughly the same amount of study time.

Section 2 and the first part of Section 3 build on notions that should be familiar to you from your previous studies.

Section 3 is slightly longer and uses the tools provided in the first two sections to prove two pivotal results: Cayley's Theorem and Cauchy's Theorem.

All three sections contain a balanced mixture of examples and more abstract results.

1 Direct products

This section describes how to construct a group called the *direct product* of two given groups, and then describes certain conditions under which a group can be regarded as the direct product of its subgroups.

1.1 The external direct product of two groups

In this subsection, we introduce a method of constructing a new group from two existing ones: their *external direct product*. This method of construction will enable us to use existing groups as building blocks for larger ones. In turn, this will enable us to describe some groups in terms of smaller and possibly less complicated groups. This construction is, therefore, a key tool in our progress towards classifying groups.

First we need the notion of the **Cartesian product** of two sets: if X and Y are two sets, then the Cartesian product $X \times Y$ is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. For example, if $X = \{1, 2, 3\}$ and $Y = \{a, b\}$ then

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

When $X = Y$, the Cartesian product $X \times Y = X \times X$ is also denoted by X^2. More generally, the Cartesian product of n sets $X_1, X_2, \ldots, X_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in X_i$ for all $i = 1, \ldots, n$.

In order to define the direct product of two groups, we need to specify the underlying set and a suitable binary operation. To understand how this is done, it will be useful to examine the familiar example of addition of vectors in the real plane $\mathbb{R} \times \mathbb{R}$ represented by the usual coordinate system.

Example 1.1 *Addition of vectors in* $\mathbb{R} \times \mathbb{R}$

We know that the real numbers with addition are a group, which we denoted by $(\mathbb{R}, +)$ in Chapter 5.

Each point in the plane is represented by an ordered pair (x, y) of real numbers. In other words, the coordinates of points in the plane are elements of the Cartesian product

$$\mathbb{R} \times \mathbb{R} = \{(x, y) : \ x \in \mathbb{R}, \ y \in \mathbb{R}\}.$$

The familiar operation of vector addition on $\mathbb{R} \times \mathbb{R}$ is defined as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Thus, vector addition is defined component by component in terms of addition in $\mathbb{R}$.

It turns out that $\mathbb{R} \times \mathbb{R}$ with addition defined as in Example 1.1 above is a group.

Exercise 1.1

Prove that the set $\mathbb{R} \times \mathbb{R}$ with the operation of vector addition is a group.

We can generalise the definitions of both the real plane as a Cartesian product and component-wise addition of real numbers.

Given two groups $(G, \circ)$ and $(H, *)$, we define the underlying set of a new group to be the Cartesian product of the sets G and H; that is, the set

In Example 1.1, $G = H = \mathbb{R}$.

$$G \times H = \{(g, h) : \ g \in G, \ h \in H\}.$$

As with $\mathbb{R} \times \mathbb{R}$, we can define an operation on this set by applying the original operations to the separate components. Generalising requires a little care because the operations for the two component groups may be different. As the first components come from G, with operation $\circ$, and the second components come from H, with operation $*$, the general definition of the new operation (which we call $\bullet$) is

In Example 1.1, $\bullet = \circ = * = +$.

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

Definition 1.2 *Direct product of two groups*

Let $(G, \circ)$ and $(H, *)$ be two groups. Their **direct product** $(G \times H, \bullet)$ is the group defined as follows.

Set The underlying set of the group is $G \times H$, the Cartesian product of the underlying sets G and H; that is,

$$G \times H = \{(g, h) : \ g \in G, \ h \in H\}.$$

Operation If (g_1, h_1) and (g_2, h_2) are elements of $G \times H$ then

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

This definition does indeed produce a group. Before we prove this, the following exercise will give you some 'hands-on' experience of direct products of groups.

Exercise 1.2

Write out the Cayley table of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. Use $+$ for the new operation.

We are now ready to prove that the direct product of any two groups is indeed a group. The proof for the general case is similar to the solution to Exercise 1.1.

To verify that $(G \times H, \bullet)$ is a group, we must check the four group axioms.

To check that the above definition of $\bullet$ produces a closed binary operation on $G \times H$ (that is, it satisfies the closure axiom), we observe the following.

Let (g_1, h_1) and (g_2, h_2) be any two elements of $G \times H$. By the definition of $G \times H$, we know that g_1 and g_2 are elements of G and that h_1 and h_2 are elements of H.

Since G is a group, it is closed under the operation $\circ$, therefore $g_1 \circ g_2$ is in G. Since H is a group, it is closed under the operation $*$, so $h_1 * h_2$ is in H. Therefore, by the definition of $\bullet$, we have

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \in G \times H.$$

The following exercise asks you to check the remaining group axioms for $(G \times H, \bullet)$.

Exercise 1.3

(a) Prove that $\bullet$ is associative (that is, check the associativity axiom).

(b) Let the identity of G be e_G and the identity of H be e_H. Prove that (e_G, e_H) is the identity of $G \times H$ (that is, check the identity axiom).

(c) Let (g, h) be an element of $G \times H$, where g has inverse g^{-1} in G and h has inverse h^{-1} in H. Prove that (g^{-1}, h^{-1}) is the inverse of (g, h) in $G \times H$ (that is, check the inverses axiom).

So far we have carefully distinguished the binary operations of the groups involved in the direct product construction. Now that we have shown that the direct product of two groups is a group, we revert to using either juxtaposition for the operations, or $+$ when both the operations are addition. Some texts refer to the **direct sum** of two groups, rather than direct product, when the groups are abelian and additive notation is used.

Exercise 1.4

Let G and H be abelian groups. Show that their direct product $G \times H$ is abelian.

1.2 Internal direct products

In some cases, a group is isomorphic to the direct product of two more of its subgroups. This is not always obvious, and in this subsection we investigate how to find out whether this is the case.

Consider the group of symmetries of the rectangle, $V = \{e, r, h, v\}$, where r is the half-turn about the centre and h and v are the reflections in the horizontal and vertical axes of symmetry. Recall also that $v = rh$. The Cayley table of V is as follows.

	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

We will show how V can be represented as a direct product of two smaller groups. More specifically, we will show that V is isomorphic to the direct product of two of its subgroups.

By Lagrange's Theorem (Chapter 5, Theorem 2.16) the only possible orders for subgroups of V are 1, 2 and 4. We aim to express V in the form $V = A \times B$, where A and B are subgroups of V. Now, by the definition of direct products of *any* two groups A and B,

$$|A \times B| = |A||B|.$$

Therefore if either A or B has order 1, then the other must have order 4 and is the whole group. However, this would not be expressing V as a product of smaller groups. Thus, it only makes sense to try to express V as the direct product of two subgroups of order 2. There are three subgroups of order 2, namely

$$H_1 = \{e, r\}, \quad H_2 = \{e, h\} \quad \text{and} \quad H_3 = \{e, v\}.$$

We pick H_1 and H_2, although any two of the three subgroups would do just as well. The Cayley table for $H_1 \times H_2$ is as follows.

	(e,e)	(r,e)	(e,h)	(r,h)
(e,e)	(e,e)	(r,e)	(e,h)	(r,h)
(r,e)	(r,e)	(e,e)	(r,h)	(e,h)
(e,h)	(e,h)	(r,h)	(e,e)	(r,e)
(r,h)	(r,h)	(e,h)	(r,e)	(e,e)

Since $rh = v$ in V, the Cayley table for V can be rewritten in the following way.

	e	r	h	rh
e	e	r	h	rh
r	r	e	rh	h
h	h	rh	e	r
rh	rh	h	r	e

You may have observed that these two tables have an entirely similar pattern. It follows that the function $\phi : H_1 \times H_2$ defined by

$$\phi : (x, y) \mapsto xy$$

is an isomorphism. Thus V can be represented as – that is, it is isomorphic to – the direct product of two of its subgroups. Since each of these subgroups is cyclic and of order 2, we can also say $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Not all attempts to decompose a group as a direct product of subgroups will work, as the following example shows.

Example 1.3 *A group that is not a non-trivial direct product*

The symmetric group S_3 has six elements:

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

This group is not abelian: consider, for example, the products $(1\,2)(1\,3)$ and $(1\,3)(1\,2)$.

If S_3 could be written as a *non-trivial* direct product – that is, as a direct product in which neither subgroup has order 1 – it would have to be as the direct product of subgroups of orders 2 and 3.

The group S_3 does possess subgroups of orders 2 and 3. For example, $H_1 = \{e, (1\,2)\}$ has order 2 and $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ has order 3.

However, any subgroup of order 2 is cyclic and is isomorphic to $\mathbb{Z}_2$. Equally, any subgroup of order 3 is cyclic and is isomorphic to $\mathbb{Z}_3$. It follows, therefore, that *any* attempt to form a direct product of such subgroups leads to a group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is abelian by Exercise 1.4 and so not isomorphic to S_3.

Example 1.3 shows that, even if subgroups of suitable orders exist, a group may not be isomorphic to a direct product of these subgroups.

In fact, there are precise conditions under which a group is isomorphic to a direct product of two of its subgroups. These conditions form the content of Theorem 1.5 below.

We determine these conditions in two stages: first we establish necessary conditions on the subgroups and then we show that these conditions are also sufficient.

This discussion will be the proof of the first half of Theorem 1.5.

We start by showing that if a group G is the direct product of two of its subgroups, then there are certain restrictions on the subgroups.

So assume that H_1 and H_2 are subgroups of a group G and that $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism. We consider, in turn, the consequences of ϕ being onto, one–one and satisfying the morphism property.

The image set of ϕ consists of all products $h_1 h_2$ of an element of H_1 and an element of H_2. Hence, as ϕ is onto, every element of G is expressible in

this form. Using the notation $H_1H_2 = \{h_1h_2 : \ h_1 \in H_1, \ h_2 \in H_2\}$, this says that we must have $G = H_1H_2$. In other words, every element of G is the product of an element of H_1 with an element of H_2. Summing up, we have the following result.

If ϕ is an isomorphism, then $G = H_1H_2$.

Let us now look at the consequences of ϕ being one–one. Assume that $\phi(h_1, h_2) = \phi(k_1, k_2)$. Then we know that

$$(h_1, h_2) = (k_1, k_2),$$

which, by the definition of an ordered pair, implies that $h_1 = k_1$ and $h_2 = k_2$.

Strictly, the correct notation for expressions like $\phi(h_1, h_2)$ is $\phi((h_1, h_2))$. However, for ease of notation we will avoid double brackets where no ambiguity arises and simply write $\phi(h_1, h_2)$.

So $\phi(h_1, h_2) = \phi(k_1, k_2)$ means that $h_1h_2 = k_1k_2$. In other words, the fact that ϕ is one–one means that

$$h_1h_2 = k_1k_2 \quad \text{implies} \quad h_1 = k_1 \text{ and } h_2 = k_2.$$

Thus, because ϕ is one–one, each element of G can be expressed as a *unique* product of the form h_1h_2 with $h_1 \in H_1$ and $h_2 \in H_2$.

Exercise 1.5

Show that the fact that ϕ is one–one implies that $H_1 \cap H_2 = \{e\}$.

Hint: use the fact that $h = he = eh$ for any $h \in G$.

The result of the previous exercise tells us the following.

If ϕ is an isomorphism, then $H_1 \cap H_2 = \{e\}$.

For any two elements (h_1, h_2) and (k_1, k_2) of the direct product, the morphism property of ϕ gives

$$\begin{aligned}
&\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2) \\
&\Rightarrow \phi(h_1k_1, h_2k_2) = (h_1h_2)(k_1k_2) \\
&\Rightarrow h_1k_1h_2k_2 = h_1h_2k_1k_2 \\
&\Rightarrow k_1h_2 = h_2k_1, \qquad \text{using the left and right cancellation rules.}
\end{aligned}$$

What this means is that every element of H_1 commutes with every element of H_2.

We now show that we can deduce that H_1 is a normal subgroup of G. To do so, we show that $aH_1a^{-1} \subseteq H_1$ for each $a \in G$. Then H_1 is normal by Proposition 3.7 in Chapter 5.

So suppose that $a \in G$. Since we now know that $G = H_1H_2$, we can write $a = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Now, any element of aH_1a^{-1} is of the form aha^{-1}, where $h \in H_1$. So

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1hh_2h_2^{-1}h_1^{-1} \qquad \text{(since } h \in H_1 \text{ and } h_2 \in H_2 \text{ commute)} \\ &= h_1hh_1^{-1} \in H_1 \qquad \text{(since } h, h_1, h_1^{-1} \in H_1\text{)}. \end{aligned}$$

Thus $aH_1a^{-1} \subseteq H_1$ as required.

The following exercise asks you to show that H_2 is also a normal subgroup of G.

Exercise 1.6

Prove that, for any $a \in G$,

$$aH_2a^{-1} \subseteq H_2.$$

Exercise 1.6 and the discussion preceding it give the following result.

If ϕ is an isomorphism, then both H_1 and H_2 are normal subgroups of G.

Summing up, if $\phi : H_1 \times H_2 \to G$ defined by

$$\phi : (h_1, h_2) \mapsto h_1h_2$$

is an isomorphism, then all three of the following conditions are satisfied:

(a) $G = H_1H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

This completes the proof of the first half of Theorem 1.5 below. Before we state the theorem and complete its proof, we introduce the standard terminology that is used when a group can be expressed as a direct product of subgroups.

Definition 1.4 *Internal direct product*

Let G be a group and let H_1 and H_2 be subgroups of G. Then G is the **internal direct product** of H_1 and H_2 if the map

$$\begin{aligned} \phi &: H_1 \times H_2 \to G \\ \phi &: (h_1, h_2) \mapsto h_1h_2 \end{aligned}$$

is an isomorphism.

The direct product $H_1 \times H_2$ in Definition 1.4 is 'internal' in that H_1 and H_2 are subgroups of G. The next theorem gives necessary and sufficient

conditions for a group to be the internal direct product of two given subgroups.

Theorem 1.5 *Internal Direct Product Theorem*

If H_1 and H_2 are subgroups of a group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of H_1 and H_2.

Proof As remarked above, we have proved that the conditions are necessary; that is, we have proved that if ϕ is an isomorphism, then the three conditions hold. For sufficiency, we need to prove that, if the three conditions hold, then ϕ is an isomorphism.

The three conditions, in turn, give that ϕ is onto, one–one and has the morphism property.

To see that ϕ is onto, recall that $G = H_1 H_2$. Then every $g \in G$ can be written as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$. Hence $g = \phi(h_1, h_2)$ and ϕ is onto.

We now check that ϕ is one–one. Suppose that

$$\phi(h_1, h_2) = \phi(k_1, k_2).$$

Then $h_1 h_2 = k_1 k_2$ for $h_1, k_1 \in H_1$ and $h_2, k_2 \in H_2$. So

$$k_1^{-1} h_1 = k_2 h_2^{-1}.$$

But the left-hand side is an element of H_1 and the right-hand side is an element of H_2. Since both sides are equal, they belong to both H_1 and H_2 and, hence, to the intersection $H_1 \cap H_2$.

However, $H_1 \cap H_2 = \{e\}$.

Thus $k_1^{-1} h_1 = k_2 h_2^{-1} = e$.

It follows that $h_1 = k_1$ and $h_2 = k_2$, and so $(h_1, h_2) = (k_1, k_2)$. Thus ϕ is one–one.

Checking the morphism property is slightly more involved. Let (h_1, h_2) and (k_1, k_2) be elements of $H_1 \times H_2$. We want to show that

$$\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1, h_2)\phi(k_1, k_2).$$

But $\phi((h_1, h_2)(k_1, k_2)) = \phi(h_1 k_1, h_2 k_2) = h_1 k_1 h_2 k_2$, and
$\phi(h_1, h_2)\phi(k_1, k_2) = h_1 h_2 k_1 k_2$,

so the morphism property in this case is equivalent to

$$h_1k_1h_2k_2 = h_1h_2k_1k_2;$$

that is, after using the cancellation laws, to

$$k_1h_2 = h_2k_1.$$

Now consider the product

$$k_1h_2k_1^{-1}h_2^{-1} \in G.$$

Since h_2 is in H_2, so is h_2^{-1}. Since H_2 is normal in G, we have that $k_1h_2k_1^{-1}$ is in H_2. Therefore $k_1h_2k_1^{-1}h_2^{-1}$ is in H_2.

Similarly, $h_2k_1^{-1}h_2^{-1} \in H_1$, so $k_1h_2k_1^{-1}h_2^{-1} \in H_1$.

Therefore $k_1h_2k_1^{-1}h_2^{-1} \in H_1 \cap H_2$. But since $H_1 \cap H_2 = \{e\}$, we have

$$k_1h_2k_1^{-1}h_2^{-1} = e,$$

which is equivalent to $k_1h_2 = h_2k_1$, and therefore also to the morphism property.

This concludes the proof that if conditions (a), (b) and (c) hold, then ϕ is an isomorphism. ■

Theorem 1.5 gives another reason why S_3 is not the direct product of two subgroups isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$: while $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ is a normal subgroup of order 3, we know that S_3 has no normal subgroup of order 2.

Exercise 1.7

Consider the cyclic group $\mathbb{Z}_6$ and denote its underlying set by $\{e, a, a^2, a^3, a^4, a^5\}$. Show that $\mathbb{Z}_6$ has normal subgroups of orders 2 and 3 that satisfy the conditions of Theorem 1.5. Deduce that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

The result you are asked to prove in the following exercise is implicit in the proof of the morphism property for ϕ in Theorem 1.5: in any internal direct product $G \cong H \times K$, the subgroups H and K satisfy a commutativity condition, in the sense that every element of H commutes with every element of K.

Exercise 1.8

Let $G \cong H \times K$ be the internal direct product of subgroups H and K of G. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

Let G and H be two groups with identities e_G and e_H respectively. Then the set

$$\widehat{G} = \{(g, e_H) : g \in G\}$$

is the subset of the direct product $G \times H$ that contains all pairs where the second element is the identity in H. It is not difficult to show – though we will not do so here – that $\widehat{G}$ is a subgroup of $G \times H$ that is isomorphic to G. Similarly, the set

$$\widehat{H} = \{(e_G, h) : h \in H\}$$

forms a subgroup of $G \times H$ that is isomorphic to H.

Then the direct product $G \times H$ is also the internal direct product of its subgroups $\widehat{G}$ and $\widehat{H}$. Thus, the distinction between the external and internal direct products of two groups is simply an indication of whether we regard the factor groups as subgroups of the product group. In the rest of Book B we will usually drop this distinction and simply refer to a *direct product* even when we work with an internal direct product.

Before we move on, it will be useful to consider direct products of more than two groups.

Theorem 1.6

If A, B and C are groups, then:

(a) $A \times B \cong B \times A$

(b) $A \times (B \times C) \cong (A \times B) \times C$.

Proof

(a) Consider the function $\phi : A \times B \to B \times A$ defined by

$$\phi : (a, b) \mapsto (b, a).$$

We claim that ϕ is an isomorphism.

To show that ϕ is one–one, suppose that $\phi(a_1, b_1) = \phi(a_2, b_2)$. Then $(b_1, a_1) = (b_2, a_2)$ by the definition of ϕ. Hence $b_1 = b_2$ and $a_1 = a_2$ by the definition of ordered pairs, and so

$$(a_1, b_1) = (a_2, b_2),$$

which shows that ϕ is one–one.

If (b, a) is any element of the codomain $B \times A$, then $b \in B$ and $a \in A$, so $(a, b) \in A \times B$ and $\phi(a, b) = (b, a)$. Hence ϕ is onto.

To check the morphism property, let (a_1, b_1) and (a_2, b_2) be any two elements of $A \times B$. Then

$$\begin{aligned} \phi((a_1, b_1)(a_2, b_2)) &= \phi(a_1 a_2, b_1 b_2) \\ &= (b_1 b_2, a_1 a_2) \\ &= (b_1, a_1)(b_2, a_2) \\ &= \phi(a_1, b_1)\phi(a_2, b_2). \end{aligned}$$

This completes the proof that $A \times B \cong B \times A$.

(b) You are asked to prove the second part of the theorem in the following exercise. ■

Exercise 1.9

Show that the function

$$\begin{aligned} \psi : A \times (B \times C) &\to (A \times B) \times C \\ \psi : \quad (a, (b, c)) &\mapsto \quad ((a, b), c) \end{aligned}$$

is an isomorphism.

The first part of Theorem 1.6 says that if we alter the order of the factor groups in a direct product, we obtain an isomorphic group.

The second part of Theorem 1.6 says that the bracketing of terms in a direct product of three (or more) groups is unnecessary.

So, just as for, say, the multiplication of integers, these 'commutative' and 'associative' laws mean that a direct product of two or more groups may be written in any order, without the need for brackets, since all such expressions produce isomorphic groups. Theorems 1.5 and 1.6 give us the following result concerning the direct product of a finite number of subgroups of a group G. The full proof is omitted.

Corollary 1.7

If H_i are subgroups of a group G for $i = 1, \ldots, n \in \mathbb{N}$, $n \geq 2$, then

$$\begin{aligned} \phi\colon \quad H_1 \times H_2 \times \cdots \times H_n &\to G \\ \phi : (h_1, h_2, \ldots, h_n) &\mapsto h_1 h_2 \cdots h_n \end{aligned}$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2 \cdots H_n$

(b) $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$ for $1 \leq i \leq n$

(c) $H_1, H_2, \ldots, H_n$ are normal subgroups of G.

In particular, when these three conditions are satisfied, G is the internal direct product of $H_1, H_2, \ldots, H_n$.

Notice that condition (b) is stronger than requiring that $H_i \cap H_j = \{e\}$ for $i \neq j$. The next example shows that this extra strength is needed.

Example 1.8 *The Klein group*

Let G be the Klein group,

$$G = \Gamma(\square) = \{e, r, h, v\}.$$

Let $H_1 = \{e, r\}, H_2 = \{e, h\}$ and $H_3 = \{e, v\}$. Then:

- $e = eee$, $r = ree$, $h = ehe$ and $v = eev$ and so condition (a) from Corollary 1.7 holds
- $H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3 = \{e\}$
- since G is abelian, H_1, H_2, H_3 are all normal in G.

However $G \ncong H_1 \times H_2 \times H_3$, since the order of G is 4, whereas the order of $H_1 \times H_2 \times H_3$ is 8.

Note that condition (b) in Corollary 1.7 does not hold here, since

$$H_1 \cap H_2 H_3 = H_1 \cap \{e, h, v, r\} = \{e, r\}.$$

When a group G has two subgroups H and K with trivial intersection, we can say quite a lot about the product HK and its relation to the direct product $H \times K$.

Recall that $HK = \{hk : h \in H \text{ and } k \in K\}$.

Proposition 1.9

Let G be a group with subgroups H and K such that $H \cap K = \{e\}$. Then:

(a) If H and K have finite orders r and s respectively, then HK has rs distinct elements. In particular, if $rs = |G|$ then $G = HK$.

(b) If $kh = hk$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G with $HK \cong H \times K$.

Proof

(a) Suppose that $h_1 k_1 = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$h_2^{-1} h_1 = k_2 k_1^{-1} = e$$

since $H \cap K = \{e\}$. Thus $h_2 = h_1$ and $k_2 = k_1$. This means that HK must have $|H| \times |K| = rs$ distinct elements.

(b) We first apply the subgroup criterion in Proposition 2.4 of Chapter 5 to show that HK is a subgroup of G. It is clear that HK is non-empty, so we only need to check that for any elements x, $y \in HK$ the product $x^{-1}y$ is again in HK.

Suppose $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} x^{-1}y &= (h_1k_1)^{-1}h_2k_2 \\ &= k_1^{-1}h_1^{-1}h_2k_2 \\ &= h_1^{-1}h_2k_1^{-1}k_2, \end{aligned}$$

since elements of H commute with elements of K.

But $h_1^{-1}h_2 \in H$ and $k_1^{-1}k_2 \in K$ (because H and K are both subgroups), therefore the product $h_1^{-1}h_2k_1^{-1}k_2 = x^{-1}y$ is in HK, as required.

Thus HK is a subgroup of G.

Now, since $hk = kh$ for all $h \in H$ and $k \in K$, we have

$$\begin{aligned} hkh^{-1} &= k \in K \quad \text{and} \\ khk^{-1} &= h \in H, \end{aligned}$$

so H and K are both normal subgroups of HK.

Hence, since $H \cap K = \{e\}$, we can apply Theorem 1.5 with $HK = G$ to show that $HK \cong H \times K$ as required. ■

The next exercise gives a useful tip for working with direct products of two groups inside abelian groups.

Exercise 1.10

Let G be an abelian group, and let H_1, H_2 be subgroups of G with

$$H_1 \cap H_2 = \{1\}.$$

Show that if $h_1 \in H_1$ and $h_2 \in H_2$ are such that $h_1h_2 = 1$, then $h_1 = 1$ and $h_2 = 1$.

Finally, we include a result about direct products of direct products.

Proposition 1.10

Let H, K be subgroups of G, and H_1, H_2 be subgroups of H. Suppose that $G \cong H \times K$ and $H \cong H_1 \times H_2$. Then $G \cong H_1 \times H_2 \times K$.

Proof We show that the three conditions in Corollary 1.7 hold for G, H_1, H_2 and K.

(a) Since $G \cong H \times K$, we have that $G = HK$ and since $H \cong H_1 \times H_2$, we have that $H = H_1H_2$. It follows that $G = H_1H_2K$.

(b) Since $G \cong H \times K$, we have that $H \cap K = \{e\}$ and so $H_1H_2 \cap K = \{e\}$.

Since $H \cong H_1 \times H_2$, we have $H_1 \cap H_2 = \{e\}$. Suppose $g \in H_1K \cap H_2$. Then

$$g = h_1k = h_2 \qquad (*)$$

for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$.

But then $k = h_1^{-1}h_2 \in H$ and so $k \in H \cap K$. Thus $k = e$, and $h_1 = h_2$. But $h_1 = h_2$ implies that $h_1 = h_2 = e$ because $H_1 \cap H_2 = \{e\}$. Then equation $(*)$ implies $g = e$, and so

$$H_1K \cap H_2 = \{e\}.$$

The proof that $H_2K \cap H_1 = \{e\}$ is similar.

(c) Since $G \cong H \times K$, by Theorem 1.5 we have that K is normal in G. From Exercise 1.8 we know that:

- $hk = kh$ for all $h \in H$ and $k \in K$
- $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

Now let $h \in H_1$ and $g \in G$. We can write $g = h_1h_2k$ for some $h_1 \in H_1, h_2 \in H_2$ and $k \in K$. Then

$$\begin{aligned} ghg^{-1} &= h_1h_2khk^{-1}h_2^{-1}h_1^{-1} \\ &= h_1h_2h_2^{-1}kk^{-1}hh_1^{-1} \\ &= h_1hh_1^{-1} \in H_1. \end{aligned}$$

Thus H_1 is normal in G. Similarly, H_2 is normal in G.

We have shown that the three conditions in Corollary 1.7 are satisfied and hence that $G \cong H_1 \times H_2 \times K$. ■

2 Cyclic groups

We defined cyclic groups in Subsection 1.4 of Chapter 5. This section describes the key properties of their structure, starting with a complete description of all cyclic groups.

We will often retain multiplicative notation despite the fact that we know that cyclic groups are abelian.

2.1 The classification of cyclic groups

We are already in a position to describe fully all cyclic groups up to isomorphism. We do so by showing that any cyclic group is isomorphic to one of a list of concrete examples of groups. In fact, the concrete examples are

$$(\mathbb{Z}, +) \quad \text{and} \quad (\mathbb{Z}_n, +_n)$$

for each positive integer n.

$\mathbb{Z}$ is also generated by -1.

The cyclic group with which you are most familiar is $(\mathbb{Z}, +)$, which is generated by the element 1.

Theorem 2.1

(a) All infinite cyclic groups are isomorphic to $(\mathbb{Z}, +)$.

(b) A finite cyclic group of order n is isomorphic to the quotient group $\mathbb{Z}/n\mathbb{Z}$, which is $(\mathbb{Z}_n, +_n)$.

Proof

(a) Let G be an infinite cyclic group. Then G has a generator, a say, so every element of G can be written as a^n for some $n \in \mathbb{Z}$.
Define the function $\phi : G \to \mathbb{Z}$ by

$$a^n \mapsto n.$$

We claim that ϕ is an isomorphism. Since $a^n = a^m \Rightarrow n = m$, we have that ϕ is well defined. For any $m \in \mathbb{Z}$, $\phi(a^m) = m$, so ϕ is onto.

Since $\phi(a^n) = \phi(a^m) \Rightarrow n = m$, we have that

$$\phi(a^n) = \phi(a^m) \Rightarrow a^n = a^m,$$

so ϕ is one–one.

Finally, we check the morphism property, that is, we check that $\phi(a^n) + \phi(a^m) = \phi(a^n a^m)$. The key to this is that we have been using standard power notation when considering elements of groups; that is, we write

$$\underbrace{aa\cdots a}_{n \text{ times}} \text{ as } a^n, \quad \text{and} \quad \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}} \text{ as } a^{-n}.$$

Thus, the familiar power laws apply to products of elements of G, and we get

$$\phi(a^n) + \phi(a^m) = n + m = \phi(a^{n+m}) = \phi(a^n a^m).$$

Therefore the morphism property holds.

(b) Let G be a finite cyclic group of order n. Then G has a generator, a say, so every element of G can be written as a^s for some $s \in \mathbb{Z}$ and, moreover, $a^n = e$.

Now, by the Division Algorithm (see Book A, Chapter 1, Theorem 4.1) we have that $s = kn + r$ where $0 \leq r < n$. Thus

$$a^s = a^{kn+r} = (a^n)^k a^r = a^r.$$

Hence $G = \{e, a, a^2, \ldots, a^{n-1}\}$, and these elements are distinct.

Define the function $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ by

$$a^r \mapsto r + n\mathbb{Z}.$$

We show that ϕ is an isomorphism. It is clear that ϕ is onto. To show that ϕ is one–one, we need to check that $\phi(a^r) = \phi(a^s) \Rightarrow a^r = a^s$. Now

$$\begin{aligned}\phi(a^r) = \phi(a^s) &\Rightarrow r + n\mathbb{Z} = s + n\mathbb{Z} \\ &\Rightarrow r - s = kn \text{ for some } k \in \mathbb{Z} \\ &\Rightarrow r = s + kn \\ &\Rightarrow a^r = a^{s+kn} = a^s a^{kn} = a^s \ \ (\text{since } a^n = e),\end{aligned}$$

as required.

Finally, we need to show the morphism property. Suppose that $r, s \in \mathbb{Z}$. Let $t \in \mathbb{Z}$ be such that $0 \leq t < n$ and $t \equiv r + s \pmod{n}$. Then

$$\begin{aligned}\phi(a^r a^s) &= \phi(a^{r+s}) \\ &= \phi(a^t) \qquad (\text{since } r + s = t + kn \text{ for some } k \in \mathbb{Z}) \\ &= t + n\mathbb{Z} \\ &= r + n\mathbb{Z} + s + n\mathbb{Z} \\ &= \phi(a^r) + \phi(a^s),\end{aligned}$$

so the morphism property holds. ■

2.2 Subgroups and quotient groups of cyclic groups

Chapter 5 showed that subgroups and quotient groups of abelian groups are abelian. A natural question arises as to whether the same is true if 'abelian' is replaced by 'cyclic'. The answer is yes, as will be shown in this subsection.

Although we know, from Theorem 2.1, that cyclic groups can be written in a specific form, namely as $\mathbb{Z}$ or $\mathbb{Z}_n$, it is sometimes convenient to view them in a more abstract way and in multiplicative notation. This more abstract view is adopted in this subsection.

We begin by looking at quotients of cyclic groups.

Theorem 2.2 *Quotients of cyclic groups*

(a) Let G be a cyclic group and let $\phi : G \to H$ be a homomorphism. Then $\phi(G)$ is cyclic.

(b) Let G be a cyclic group generated by a and let H be a subgroup of G. Then the quotient group G/H is cyclic and generated by the coset aH.

Proof

(a) Since G is cyclic, it has a generator g, say. We claim that $\phi(g) \in H$ generates $\phi(G)$.

Let $h \in \phi(G)$. Then $h = \phi(a)$ for some $a \in G$. Since g generates G we know that $a = g^n$ for some $n \in \mathbb{Z}$. Hence

$$h = \phi(a) = \phi(g^n) = (\phi(g))^n.$$

Thus we have shown that every element of $\phi(G)$ can be written in the form $(\phi(g))^n$ for some $n \in \mathbb{Z}$, and so $\phi(G)$ is cyclic with generator $\phi(g)$, as required.

(b) We must show that every element of G/H is of the form $(aH)^k$ for some $k \in \mathbb{Z}$.

Suppose that gH is any element of G/H. Then, since G is generated by a, we know that $g = a^k$ for some integer k. But $(aH)^k = (a^k)H = gH$. Hence aH generates G/H. ■

Before proving that every subgroup of a cyclic group is cyclic, you are asked to work through an exercise that should help you understand what is happening.

Exercise 2.1

Let G be a cyclic group generated by a and let H be a non-trivial subgroup of G. Each element of H must be of the form a^k with $k \geq 0$. Among the elements of H, choose the one with the smallest non-zero exponent and let this exponent be m. Since H is non-trivial, such an m exists.

(a) Suppose that a^k is an element of H. Show that m divides k and hence that $H = \langle a^m \rangle$.

Assume now that G is a finite cyclic group of order n – that is, a has order n.

(b) Deduce that m divides n.

(c) If $n = mq$, show that the order of H is q.

Hint: in part (a), use the Division Algorithm (Book A, Chapter 1, Theorem 4.1).

Exercise 2.1 is a major step towards the proof that every subgroup of a cyclic group is cyclic.

Theorem 2.3

Let G be a cyclic group and let H be a subgroup of G. Then H is cyclic.

Proof If H is the trivial subgroup, that is $H = \{e\}$, then H is generated by e and so it is cyclic.

We therefore consider the case when $H \neq \{e\}$, so that H contains a^t for some integer $t \neq 0$. Then H also contains $a^{-t} = (a^t)^{-1}$. As one of t and $-t$ must be positive, H contains a^k for some positive integer k and we can choose m to be the least such positive integer. Then $H = \langle a^m \rangle$ by Exercise 2.1, and so H is cyclic and generated by a^m. ■

Interpreting this result for the infinite cyclic group $\mathbb{Z}$, using additive notation, gives the following corollary.

Corollary 2.4

The subgroups of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$, $n \geq 0$.

Proof By Theorem 2.3, every subgroup of $\mathbb{Z}$ is cyclic. The cyclic subgroups of $\mathbb{Z}$ are those generated by an element of $\mathbb{Z}$, that is, those of the form $\{nz : z \in \mathbb{Z}\} = n\mathbb{Z}$ for some $n \in \mathbb{Z}, n > 0$, as required. ■

We can summarise the results in Exercise 2.1 and Theorem 2.3 as follows. If

$$G = \langle a : a^n = e \rangle$$

is a finite cyclic group of order n and H is a subgroup of G, then:

- H is cyclic
- H is generated by a^m, where m is the smallest positive exponent of a such that $a^m \in H$
- m divides n
- if $n = mq$ then H has order q.

We have shown that every subgroup of a cyclic group is also cyclic. In fact where the group is finite, we will do rather more. As we have seen, Lagrange's Theorem states that, for finite groups, the order of a subgroup must divide the order of the group. For finite *cyclic* groups we can prove a strong converse to Lagrange's Theorem: for every divisor of the order of the group, not only is there a subgroup having that number of elements, but also this subgroup is unique.

Theorem 2.5 *Subgroups of cyclic groups*

Let $G = \langle a \rangle$ be a finite cyclic group of order n, so that a has order n. If q is a factor of n with $n = mq$, then G has a unique subgroup of order q that is generated by the element a^m.

Proof

We start by proving the existence of subgroups whose orders correspond to factors of the order of the group.

Let H be the subgroup $H = \langle a^m \rangle$. In Exercise 2.1, you showed that the order of H is q. Thus, given a factor q of n, the subgroup generated by a^m, where $n = mq$, has order q.

Finally, we show that the subgroup corresponding to the factor q of n is unique.

Suppose that $n = mq$. Then we know that there *is* a subgroup $\langle a^m \rangle$ of order q. Let H be any subgroup of order q. From Exercise 2.1 and Theorem 2.3, we know that H is cyclic and generated by a^l, where l is the least positive exponent of a occurring among the elements of H. Furthermore, the order of H is k, where $n = lk$. But the order of H is q, so $k = q$ and $mq = n = lk = lq$, and, therefore, $m = l$. Thus H is the subgroup generated by a^m.

This completes the proof of Theorem 2.5. ■

Theorem 2.5 can be regarded as a strong converse to Lagrange's Theorem for cyclic groups. We say 'strong' because not only is there a subgroup for every factor of the order of the group, but, in addition, this subgroup is unique.

Later we will investigate the effect of relaxing the assumptions about the group G. We will first consider the case where G is finite and abelian (instead of cyclic) and then go on to relax the condition further to merely finite. At each stage we will still obtain some sort of converse to Lagrange's Theorem; but, as the conditions on G are relaxed, the conclusions become weaker, although still useful.

We conclude this subsection by interpreting the results that we have obtained so far for our standard finite cyclic groups, that is, the groups $\mathbb{Z}_n$.

At this point, a word is in order about how we think of $\mathbb{Z}_n$. In Theorem 2.1, the group $\mathbb{Z}_n$ was defined as the quotient group $\mathbb{Z}/n\mathbb{Z}$. However, in practice we think of $\mathbb{Z}_n$ as the set $\{0, 1, \ldots, n-1\}$, with addition carried out modulo n.

Since the order of $\mathbb{Z}_n$ is n, by Theorem 2.5 there is a subgroup corresponding to each factor of n. That is, if q is a factor of n, then $\mathbb{Z}_n$ has a cyclic subgroup of order q. Theorem 2.1 tells us that this subgroup must be isomorphic to $\mathbb{Z}_q$.

Moreover, we know a generator of the subgroup. Since $\mathbb{Z}_n$ is generated by 1, the subgroup of order q is generated by $m = \frac{n}{q}$.

Exercise 2.2

(a) Write down the orders of the subgroups of $\mathbb{Z}_{24}$.

(b) For each such subgroup:

(i) state to which $\mathbb{Z}_k$ it is isomorphic

(ii) by using the remark above about how we think of the groups $\mathbb{Z}_n$, give an explicit list of its elements.

The interpretation of our results about quotient groups is also seen quite easily: for each factor q of n, there is a subgroup of $\mathbb{Z}_n$ of order q. This subgroup is normal. The corresponding quotient group is cyclic, by Theorem 2.2, and it has order

$$\frac{|\mathbb{Z}_n|}{q} = \frac{n}{q}.$$

Hence the quotient group $\mathbb{Z}_n/\mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{\frac{n}{q}}$.

2.3 Direct products of cyclic groups

In this subsection we will apply the direct product ideas from Section 1 of this chapter to cyclic groups.

We recall some terminology and results about integers. You saw the details in Book A, Chapter 1, Section 4, so here we restate the results that we need without proof.

Let m and n be two positive integers and let $p_1, p_2, \ldots, p_k$ be the prime numbers occurring in either of their prime factorisations. Then

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

where a_i or b_i, but not both, might be zero.

For example, if $m = 126$ and $n = 120$ then $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ and we have

$$126 = 2 \times 3^2 \times 5^0 \times 7 \text{ and } 120 = 2^3 \times 3 \times 5 \times 7^0.$$

We know that the prime factorisation of mn is

$$p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k},$$

so if p is a prime factor of mn, then p must be a prime factor of either m or n or both.

Recall that the **highest common factor** of m and n, written $\text{hcf}(m, n)$, is the largest positive integer h that is a factor of both. If c_i is the smaller of a_i and b_i for each i, then h has prime factorisation

$$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}.$$

For example, $\text{hcf}(126, 120) = 2^1 \times 3^1 \times 5^0 \times 7^0 = 2 \times 3 = 6$.

The **least common multiple** of m and n, written $\text{lcm}(m, n)$, is the smallest positive integer l that is a multiple of both m and n. If d_i is the larger of a_i and b_i for each i, then l has prime factorisation

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

For example, $\text{lcm}(126, 120) = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

Two positive integers m and n are said to be **coprime** if their highest common factor is 1.

Proposition 2.6

Let m and n be two positive integers and let $h = \text{hcf}(m, n)$ and $l = \text{lcm}(m, n)$. Then:

(a) The product of m and n is the product of their highest common factor and least common multiple, that is, $mn = hl$.

(b) If m and n are coprime then their least common multiple is mn.

(c) There are integers a and b such that $am + bn = \text{hcf}(a, b)$. In particular, if m and n are coprime there are integers a and b such that $am + bn = 1$.

This proposition combines the results from Proposition 4.7, Lemma 4.9 and Proposition 4.15 of Book A, Chapter 1.

The results in Proposition 2.6 turn out to be relevant when we calculate the order of the element of a direct product. You can tackle the following exercise using direct calculation, but we will shortly prove a result that will avoid the need for calculations.

Exercise 2.3

(a) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$?

(b) What is the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$?

As promised, we now prove some results that enable us to avoid direct calculations when determining the order of an element in a direct product. The following lemma concerns the order of two commuting elements in any group.

Lemma 2.7

Let a and b be elements of finite orders m and n respectively in a group G. Suppose that $ba = ab$ and that $\langle a \rangle \cap \langle b \rangle = \{e\}$ (that is, the only element of G that can be written both as a power of a and as a power of b is e).

Then the order of ab is the least common multiple of m and n.

Proof Let $l = mp = nq$ be the least common multiple of m and n. Since a and b commute, we have that $(ab)^r = a^r b^r$ for any integer r. Then

$$(ab)^l = a^l b^l = a^{mp} b^{nq} = (a^m)^p (b^n)^q = e^p e^q = e,$$

so the order of ab is at most l. Now let $k > 0$ and suppose that $(ab)^k = e$. Then $a^k b^k = e$ so $a^k = b^{-k}$. But then $a^k \in \langle a \rangle \cap \langle b \rangle$ so $a^k = e$. Similarly, $b^k = e$. By Proposition 4.5 of Chapter 5, we have that k is a common multiple of m and n, and so $k \geq l$. Thus the order of ab is at least l. We have already seen that the order of ab is at most l, so it must be l. ■

Exercise 2.4

Let G be an abelian group and let $g_1, g_2, \ldots, g_r$ be elements of G that have distinct prime orders $p_1, p_2, \ldots, p_r$ respectively. Show that the order of $g_1 g_2 \cdots g_r$ is $p_1 p_2 \cdots p_r$.

Proposition 2.8

Let G, A, B be groups with $G = A \times B$. Suppose that $a \in A$ has order m and $b \in B$ has order n. Then the order of (a, b) is the least common multiple of m and n.

Proof We consider the elements (a, e) and (e, b) in $A \times B$ and check the hypotheses of Lemma 2.7. Firstly, $(a, e)(e, b) = (a, b) = (e, b)(a, e)$. Secondly $\langle (a, e) \rangle = \{(a^k, e) : k = 0, \ldots, m-1\}$ and $\langle (e, b) \rangle = \{(e, b^k) : k = 0, \ldots, n-1\}$, so that

$$\langle (a, e) \rangle \cap \langle (e, b) \rangle = \{(e, e)\}.$$

Since both hypotheses hold, we can conclude that the order of (a, b) is the least common multiple of m and n as required. ■

There is one more result about orders of elements in any group G that will be useful.

Proposition 2.9

If $g \in G$ has order n, then the order of g^m is

$$\frac{l}{m} = \frac{n}{h},$$

where l is the least common multiple of m and n, and h is the highest common factor of m and n. In particular, if m is a factor of n then the order of g^m is $\frac{n}{m}$.

Proof The order of g^m is the least positive integer k such that $g^{mk} = e$. By Exercise 4.7 of Chapter 5, we know that $g^{mk} = e$ precisely when mk is also a multiple of n. So k is the least positive integer such that mk is a multiple of n, hence mk is the least common multiple of m and n. Then $k = \frac{l}{m}$.

Since $mn = hl$ by Proposition 2.6(a), we also have

$$|g^m| = \frac{l}{m} = \frac{n}{h},$$

as required. ■

We can now proceed to consider direct products of cyclic groups. Firstly, we note that, as observed in Subsection 1.2, irrespective of whether the groups are cyclic or not, the order of the direct product of two finite groups is the product of the orders of the individual groups.

Secondly, if the groups concerned are cyclic, then they are abelian, and hence, by Exercise 1.4, so is their direct product.

We can now also use Proposition 2.8 to obtain results of this kind: the order of $(1, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$ is the least common multiple of the order of 1 in $\mathbb{Z}_2$ and the order of 1 in $\mathbb{Z}_3$. Since these orders are 2 and 3, with least common multiple 6, $(1, 1)$ has order 6.

On the other hand, we also know that direct products of cyclic groups are not always cyclic. For example, in Subsection 1.2 we showed that $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and V is not cyclic.

However, sometimes the direct product of cyclic groups *is* cyclic. For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. In Exercise 2.3 we showed that the order of $(1, 1)$ is 6. Since this is the order of $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle$, this direct product is indeed cyclic.

So, a direct product of cyclic groups may or may not be cyclic. The aim of this subsection is to determine under what circumstances the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

Exercise 2.5

Show that both of the following direct products are cyclic.

(a) $\mathbb{Z}_3 \times \mathbb{Z}_5$

(b) $\mathbb{Z}_4 \times \mathbb{Z}_5$

In the following exercises you will meet two examples of direct products that are not cyclic even though the factor groups are.

Exercise 2.6

(a) Show that $(1, 1)$ does not generate $\mathbb{Z}_2 \times \mathbb{Z}_4$. Why is this insufficient to prove that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic?

(b) Show that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

In the solution to Exercise 2.6, we saw that the maximum order for an element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 4. We could show this directly as follows. If (a, b) is any element of the direct product $\mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$\begin{aligned} 4(a, b) &= (4a, 4b) \\ &= (0, 0). \end{aligned}$$

Exercise 2.7

Show that the order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24 and, hence, that this direct product is not cyclic.

Being able to determine the maximum order for any element in a direct product will be useful throughout this chapter, so we generalise the result in Exercises 2.6 and 2.7 in the following proposition.

Proposition 2.10

Let $G = \mathbb{Z}_m \times \mathbb{Z}_n$. Then no element of G can have order greater than the least common multiple of m and n.

Proof Let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Suppose that a has order r and b has order s. Then by Proposition 4.5 in Chapter 5, we have that r divides m and s divides n. Thus r and s both divide $l = \text{lcm}(m, n)$. Hence

$$l(a, b) = (la, lb) = (e, e).$$

Thus the order of (a, b) is at most l, as required. ■

The property in Proposition 2.10 does not necessarily hold for a direct product where the factor groups are not both cyclic.

Exercise 2.8

Let $G = S_3 \times \mathbb{Z}_3$.

(a) What is m, the maximum order of an element of S_3?

(b) What is n, the maximum order of an element of $\mathbb{Z}_3$?

(c) What is the lowest common multiple of m and n?

(d) Write down an element of order 6 in G.

The following exercise asks you to decide whether some direct products are cyclic.

Exercise 2.9

For each of the following direct products, decide whether or not it is cyclic and justify your conclusion.

(a) $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_9$

Inspecting the examples above suggests that the direct product of cyclic groups *of coprime orders* is cyclic, but if the orders are not coprime then the direct product is not cyclic. This is the content of the next theorem. However, first you are asked to attempt the following exercise, which provides part of the proof of the theorem.

Exercise 2.10

Show that, if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Theorem 2.11 *Direct products of cyclic groups*

The direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ of the cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ is cyclic if, and only if, m and n are coprime positive integers.

Proof First we prove that, if m and n are coprime, then the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

The element 1 in $\mathbb{Z}_m$ has order m and the element 1 in $\mathbb{Z}_n$ has order n. It follows by Proposition 2.8 that $(1, 1)$ has order $\text{lcm}(m, n)$. By Proposition 2.6, we have that $\text{lcm}(m, n) = mn$. Therefore the order of the element $(1, 1)$ in the direct product is mn. However, the direct product has mn elements and so it is cyclic.

We proved the converse statement in Exercise 2.10, where we showed that if m and n are not coprime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. This is equivalent to showing that if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then m and n are coprime. ■

The next corollary gives an important and useful consequence of Theorem 2.11.

Corollary 2.12

Let m and n be coprime positive integers. Then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Proof We know that the group $\mathbb{Z}_{mn}$ is cyclic and has order mn. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ also has order mn and it is cyclic by Theorem 2.11, we have that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ by Theorem 2.1(b). ■

This corollary is an example of the sort of decomposition result that is our main concern in this book. It leads to the main decomposition theorem for cyclic groups, which we prove later in this subsection.

Exercise 2.11

Show that $\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

If, in Exercise 2.11, we had decomposed 90 in a different manner, taking $90 = 9 \times 10$, for example, we would have obtained

$$\mathbb{Z}_{90} \cong \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

Other decompositions of 90 into a product of pairwise coprime factors produce corresponding direct products. However, Theorem 1.6 ensures that all the resulting direct product decompositions are isomorphic.

Exercise 2.12

Suppose that n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers. Show that

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}$ for $i = 1, \ldots, r$.

Hint: use induction on r.

The solution to Exercise 2.12 provides a decomposition theorem for finite cyclic groups, which we restate as follows.

Theorem 2.13 *Decomposition of finite cyclic groups*

If n is a positive integer with prime decomposition

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_i = p_i^{k_i}, \quad i = 1, \ldots, r.$

If we combine Theorem 2.13 with the uniqueness of prime decomposition in $\mathbb{Z}$, we see that the decomposition into cyclic groups of prime power order is unique up to isomorphism.

Since each prime power order is a factor of the order of the group, then by Theorem 2.5 each $\mathbb{Z}_{n_i}$ is (isomorphic to) a subgroup. Thus the decomposition theorem expresses the group as a direct product of normal subgroups.

All subgroups of cyclic groups are normal.

We now have a complete description of all cyclic groups, summarised in the three bullet points below.

- Firstly, we have a list of the familiar cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$ for each positive n. Every cyclic group is isomorphic to one group in this list.
- Secondly, every finite cyclic group can be written as a direct product in which every factor is a cyclic group of prime power order. These cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders. Thus the cyclic groups of prime power order form a collection of fundamental building blocks from which all finite cyclic groups can be constructed.

The fact that cyclic groups of prime power order cannot be written as direct products of cyclic groups of smaller orders is a consequence of Theorem 2.11.

- Thirdly, we know all about the subgroups of a cyclic group.
  For the infinite cyclic group, $\mathbb{Z}$, the subgroups are precisely the sets $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$, for every non-negative integer n.
  A finite cyclic group has a unique cyclic subgroup corresponding to each factor of its order.

In addition, given any group that is a direct product of cyclic groups, we can factorise it as a direct product of cyclic groups of prime power order.

Exercise 2.13

Prove that the following two groups are isomorphic by factorising each of them as a direct product of cyclic groups of prime power order:

$$\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 \quad \text{and} \quad \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}.$$

Exercise 2.14

Factorise the following groups as a direct product of cyclic groups of prime power order.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75}$

(b) $\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245}$

3 Group actions

Each element g of the dihedral group D_4 permutes the positions of vertices of the square. Given a vertex v of the square there is a vertex, which we might denote by $g \wedge v$, to which g sends v. This is an instance of a group *acting* on a set, in this case the set of vertices of the square.

This section formalises the notion of the action of a group on a set, and discusses some specific examples. When we look at a group acting on a set, we hope to gain insight into the symmetry of the set and, at the same time, to obtain a better feel for the group.

This is most obvious when the set is a geometric figure such as the square or circle and the group is its group of symmetries, but there are other significant examples in different contexts. For instance, we will look at the case where $X = \{1, 2, \ldots, n\}$ and G is the symmetric group S_n of all permutations of X, and the case where G is S_4 and X is the set of all polynomials in four variables x_1, x_2, x_3, x_4 with integer coefficients.

3.1 Actions, orbits and stabilisers

The basic idea of a group acting on a set X is that each element of G must send each element of X to another element of X in a way that is compatible with the binary operation in G. This is expressed formally in the following definition.

Definition 3.1 *Group action*

Let G be a group and X a non-empty set. A **group action** of G on X is a function $G \times X \to X$
$(g, x) \mapsto g \wedge x$
that satisfies the following conditions:

(a) $e \wedge x = x$, for all $x \in X$, where e is the identity element of G

(b) $(gh) \wedge x = g \wedge (h \wedge x)$, for all $g, h \in G$ and $x \in X$.

We also say that G **acts** on X by $\wedge$.

Here $(g, x) \mapsto g \wedge x$ simply indicates that the image of the pair (g, x) under the function is denoted by $g \wedge x$.

Note that the definition requires that $g \wedge x$ is an element of X for every $g \in G$ and $x \in X$, so g behaves like a map from X to itself, where the image of $x \in X$ under the map associated with $g \in G$ is $g \wedge x \in X$. The first property in the definition says that the effect of the identity element of G is to leave an element of X unchanged, and the second says that the combined effect of h then g on an element of X is the same as that of the product gh.

We will start by looking at some examples of group actions.

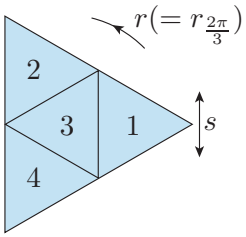

Figure 3.1 Equilateral triangle containing four triangles

Example 3.2 *Action of the group of symmetries on a plane figure*

We divide an equilateral triangle into four smaller triangles numbered $1, 2, 3, 4$ as shown in Figure 3.1.

Let X be the set of triangles $\{1, 2, 3, 4\}$ and let G be the dihedral group D_3, the group of symmetries of an equilateral triangle. Let r be the rotation about the centre of the triangle through $\frac{2\pi}{3}$ and let s be the reflection shown in Figure 3.1. Then

$$D_3 = \{e, r, r^2, s, rs, r^2s\},$$

where rs is the reflection in the line through the centres of triangles 3 and 4, and r^2s is the reflection in the line through the centres of the triangles 2 and 3. Note that $sr = r^2s$.

Then D_3 acts on X using the rule $g \wedge x = g(x)$. It is clear that $g \wedge x$ defined in this way is indeed an element of X. For example, $r \wedge 1 = r(1) = 2$. Therefore $\wedge$ defines a function from $D_3 \times X$ to X.

Below is a complete description of this action.

$e \wedge 1 = 1$	$e \wedge 2 = 2$	$e \wedge 3 = 3$	$e \wedge 4 = 4$
$r \wedge 1 = 2$	$r \wedge 2 = 4$	$r \wedge 3 = 3$	$r \wedge 4 = 1$
$r^2 \wedge 1 = 4$	$r^2 \wedge 2 = 1$	$r^2 \wedge 3 = 3$	$r^2 \wedge 4 = 2$
$s \wedge 1 = 1$	$s \wedge 2 = 4$	$s \wedge 3 = 3$	$s \wedge 4 = 2$
$rs \wedge 1 = 2$	$rs \wedge 2 = 1$	$rs \wedge 3 = 3$	$rs \wedge 4 = 4$
$r^2s \wedge 1 = 4$	$r^2s \wedge 2 = 2$	$r^2s \wedge 3 = 3$	$r^2s \wedge 4 = 1$

Since $e \wedge x = x$, condition (a) in Definition 3.1 is satisfied. Condition (b) holds since $(fg)(x) = (f)(g(x))$ for all $f, g \in D_3$ and $x \in X$.

The next example comes from polynomials in several variables. Group theory partly originated from this type of example.

Example 3.3 *Actions of symmetric groups on sets of polynomials*

Let X be the set of polynomials in three variables and let G be the symmetric group S_3. Let $f \in S_3$ and $p(x_1, x_2, x_3) \in X$. Then we define an action of S_3 on X by

$$f \wedge p(x_1, x_2, x_3) = p(x_{f(1)}, x_{f(2)}, x_{f(3)}).$$

For example, if $f = (1\ 2\ 3)$ and $p = x_1^2x_2 - x_3$ then

$$f \wedge p = x_2^2x_3 - x_1.$$

This example extends to the group S_n acting on the set P_n of polynomials in n variables. We check that this more general example is indeed a group action.

Firstly, $f \wedge p(x_1, x_2, \ldots, x_n) \in P_n$ because of the way $f \wedge p$ has been defined, so $\wedge$ does define a function $S_n \times X \to X$.

Property (a) requires that

$$e \wedge p(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n).$$

This holds because e, the identity of S_n, maps i to i for all $i = 1, \ldots, n$.

Property (b) requires that

$$g \wedge (f \wedge p(x_1, x_2, \ldots, x_n)) = gf \wedge p(x_1, x_2, \ldots, x_n).$$

Now

$$\begin{aligned} g \wedge (f \wedge p(x_1, x_2, \ldots, x_n)) &= g \wedge p(x_{f(1)}, x_{f(2)}, \ldots, x_{f(n)}) \\ &= p(x_{g(f(1))}, x_{g(f(2))}, \ldots, x_{g(f(n))}) \\ &= gf \wedge p(x_1, x_2, \ldots, x_n), \end{aligned}$$

as required. It is worth noticing that this action respects addition and multiplication of polynomials. That is, for all polynomials p and q in $x_1, x_2, \ldots, x_n$,

$$f \wedge (p + q) = f \wedge p + f \wedge q \text{ and } f \wedge (pq) = (f \wedge p)(f \wedge q).$$

For example,

$$(1\,2\,3) \wedge ((x_1 - x_2) + (x_2 - x_3)) = (1\,2\,3) \wedge (x_1 - x_3) = (x_2 - x_1), \quad \text{and}$$
$$(1\,2\,3) \wedge (x_1 - x_2) + (1\,2\,3) \wedge (x_2 - x_3) = (x_2 - x_3) + (x_3 - x_1) = (x_2 - x_1).$$

For an example involving multiplication,

$$\begin{aligned} (1\,2\,3) \wedge (x_1 - x_2)(x_2 - x_3) &= (1\,2\,3) \wedge (x_1x_2 - x_1x_3 - x_2^2 + x_2x_3) \\ &= x_2x_3 - x_2x_1 - x_3^2 + x_3x_1 \\ &= (x_2 - x_3)(x_3 - x_1) \\ &= ((1\,2\,3) \wedge (x_1 - x_2))((1\,2\,3) \wedge (x_2 - x_3)). \end{aligned}$$

Exercise 3.1

Suppose that S_4 acts on the set P_4 of polynomials in four variables in the same way as S_3 acts on the set P_3 of polynomials in three variables as described in Example 3.3. Write down the following.

(a) $(1\,2)(3\,4) \wedge x_1x_2x_3 - x_4$

(b) $(1\,2)(3\,4) \wedge x_1x_2 - x_3x_4$

(c) $(1\,2\,3\,4) \wedge x_1 + x_2 + x_3 + x_4$

Several of our basic examples of groups are groups of functions where the identity is the identity function, that is, a function that leaves every element in the domain fixed.

If X is a non-empty set and G is a group of functions from X to X, then G acts on X by the rule

$$f \wedge x = f(x).$$

We have that $f \wedge x = f(x) \in X$. We check properties (a) and (b) in Definition 3.1:

(a) $e \wedge x = e(x) = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge h(x) = g(h(x)) = (gh)(x) = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

Since both properties are satisfied, we have indeed defined a group action.

The following are examples of this kind of group action.

Example 3.4 *Actions of groups of functions*

1. The symmetric group S_n acts on $\{1, 2, \ldots, n\}$ by the rule $f \wedge x = f(x)$. For example, $(1\,4\,7) \wedge 7 = 1$.
2. The orthogonal group $\mathrm{O}(2, \mathbb{R})$ and the dihedral groups all act on $\mathbb{R}^2$. For example, if r_π denotes rotation through π then
$$r_\pi \wedge (1, 0) = (-1, 0).$$
3. Let X be a geometric figure and let G be its group of symmetries. Then G acts on X with $g \wedge x = g(x)$ for all $g \in G$ and $x \in X$. The rotation group of X also acts on X. For example, the orthogonal group $\mathrm{O}(2, \mathbb{R})$ and the special orthogonal group $\mathrm{SO}(2, \mathbb{R})$ act on the unit circle.

In the next exercise you are asked to prove an elementary consequence of the definition of group action.

Exercise 3.2

Let G be a group acting on a set X by $\wedge$ and let $x \in X$. Let $g \in G$ be such that $g \wedge x = y$. Show that $g^{-1} \wedge y = x$.

In order to prepare for an example of a group action involving the dihedral group D_6, which you met in Exercise 1.6 in Chapter 5, we gather the results of some preliminary calculations in a proposition.

Proposition 3.5

In the group D_6, let r denote a rotation through $\frac{\pi}{3}$ and s denote a reflection in an axis of symmetry, so that
$$r^6 = e, \ s^2 = e \text{ and } sr = r^5 s = r^{-1} s.$$
Then every element of D_6 can be written as $r^m s^n$ for $m = 0, \ldots, 5$ and $n = 0, 1$.

Proof We know that D_6 contains six rotations, each of which has the form $r^m = r^m s^0$ for $m = 0, \ldots, 5$. The other elements of D_6 are six reflections, which have the form $r^m s = r^m s^1$ for $m = 0, \ldots, 5$.

These elements of D_6 are all distinct, since if $r^m s = r^n$ then $r^{m-n} = s$, which is not possible. Thus we have listed all 12 elements of D_6. ■

In the next exercise you can practise manipulating products of elements of D_6. One key trick that is often used in connection with conjugation is to observe that for any elements g and h in a group G,

$$(ghg^{-1})^m = gh^m g^{-1}.$$

This is because $(ghg^{-1})^m = \underbrace{ghg^{-1}ghg^{-1}\cdots ghg^{-1}}_{m \text{ times}}$

$$= g\underbrace{h\cdots h}_{m \text{ times}}g^{-1}$$

$$= gh^m g^{-1}.$$

Exercise 3.3

Consider the group D_6 where r and s are as in Proposition 3.5. Thus

$$r^6 = e,\ s^2 = e \text{ and } sr = r^{-1}s.$$

Show that:

(a) $rs = sr^{-1}$

(b) $srs = r^{-1}$ and $sr^{-1}s = r$

(c) $sr^m s = r^{-m}$ and $sr^{-m}s = r^m$

(d) $sr^m = r^{-m}s$ and $sr^{-m} = r^m s$.

The next example that we want to explore requires some care, not because the idea is harder, but because the set X being acted on is the underlying set of the group doing the acting.

The group in this example is D_6. The set X is the set of elements of D_6. An element g of D_6 acts on an element x of X as follows:

$$g \wedge x = gxg^{-1}.$$

For example, r is an element of D_6 and rs is an element of X, so

$$\begin{aligned} r \wedge (rs) &= r(rs)r^{-1} \\ &= r^2(sr^{-1}) \\ &= r^3 s \qquad \big(\text{since } sr^{-1} = rs \text{ by Exercise 3.3}\big). \end{aligned}$$

This is called the **action of D_6 on itself by conjugation**.

Proposition 3.6

Suppose that the action $\wedge$ by D_6 on the set $X = D_6$ is defined as follows:

$$g \wedge x = gxg^{-1} \text{ for all } g \in D_6 \text{ and } x \in X.$$

Then D_6 acts on X by $\wedge$.

Proof We have that $g \wedge x = gxg^{-1} \in X = D_6$, so $\wedge$ gives a function $D_6 \times D_6 \to D_6$. We check properties (a) and (b) of Definition 3.1.

(a) $e \wedge x = exe^{-1} = exe = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge hxh^{-1} = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$. ■

In the next exercise you are asked to use the results obtained in Exercise 3.3 to give a complete description of this action. We will then tabulate the results for reference in the later discussion.

Exercise 3.4

Consider the group D_6 where r and s are as in Proposition 3.5 and let D_6 act on itself by conjugation. Show that:

(a) $r^m \wedge r^n = r^n$

(b) $r^m \wedge r^n s = r^{2m+n} s$

(c) $r^m s \wedge r^n = r^{-n}$

(d) $r^m s \wedge r^n s = r^{2m-n} s$.

We now use the fact that $0 \leq m, n \leq 5$ to complete Table 3.1.

Table 3.1 A table showing the action of D_6 on itself by conjugation

$\wedge$	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
e	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
r	e	r	r^2	r^3	r^4	r^5	r^2s	r^3s	r^4s	r^5s	s	rs
r^2	e	r	r^2	r^3	r^4	r^5	r^4s	r^5s	s	rs	r^2s	r^3s
r^3	e	r	r^2	r^3	r^4	r^5	s	rs	r^2s	r^3s	r^4s	r^5s
r^4	e	r	r^2	r^3	r^4	r^5	r^2s	r^3s	r^4s	r^5s	s	rs
r^5	e	r	r^2	r^3	r^4	r^5	r^4s	r^5s	s	rs	r^2s	r^3s
s	e	r^5	r^4	r^3	r^2	r	s	r^5s	r^4s	r^3s	r^2s	rs
rs	e	r^5	r^4	r^3	r^2	r	r^2s	rs	s	r^5s	r^4s	r^3s
r^2s	e	r^5	r^4	r^3	r^2	r	r^4s	r^3s	r^2s	rs	s	r^5s
r^3s	e	r^5	r^4	r^3	r^2	r	s	r^5s	r^4s	r^3s	r^2s	rs
r^4s	e	r^5	r^4	r^3	r^2	r	r^2s	rs	s	r^5s	r^4s	r^3s
r^5s	e	r^5	r^4	r^3	r^2	r	r^4s	r^3s	r^2s	rs	s	r^5s

This table illustrates one of the two concepts associated with group actions that we want to discuss here, the concept of an *orbit*. The columns show where each element of $X = D_6$ can be sent under the action by conjugation. Thus r can only be sent to one of r, r^5 and s can only be sent to one of s, r^2s, r^4s.

Definition 3.7 *Orbit*

If a group G acts on a set X and x is an element of X, then the **orbit** of x under G is the set

$$\mathrm{Orb}(x) = \{g \wedge x : \ g \in G\};$$

that is, the set of elements of X obtained by acting on x with the elements of G.

In our first example of a group action – that is, the action of D_3 on four triangles in Example 3.2 – we have

$$\mathrm{Orb}(1) = \{1, 2, 4\} \text{ and } \mathrm{Orb}(3) = \{3\}.$$

Exercise 3.5

Using Table 3.1, determine the orbits of all the elements of D_6 under the action of D_6 defined by $g \wedge x = gxg^{-1}$.

Note the previous exercise shows that there are only six *distinct* orbits in the action of D_6 on itself by conjugation, even though there are 12 elements.

Exercise 3.6

Suppose that S_4 acts on the set P_4 of polynomials in four variables (as in Exercise 3.1). Write down the orbits of:

(a) $x_1x_2x_3 - x_4$

(b) $x_1x_2x_3x_4$

(c) $x_1x_2 + x_3x_4$.

In the solutions to Exercises 3.5 and 3.6, you may have noticed that the orbits partition the set being acted on; that is, the orbits fill out the whole of the set being acted on and do not overlap (unless they coincide). For example, in the action of D_6 on itself by conjugation, the six sets we obtained as orbits were

$$\{e\},\ \{r, r^5\},\ \{r^2, r^4\},\ \{r^3\},\ \{s, r^2s, r^4s\},\ \{rs, r^3s, r^5s\},$$

and these six sets partition D_6.

This is not a coincidence, as the next proposition shows.

Proposition 3.8

Let G be a group acting on a set X. Then the relation $\sim$ on X defined by

$$x \sim y \quad \text{if, and only if, there is } g \in G \text{ such that } x = g \wedge y$$

is an equivalence relation.

Proof For any $x \in X$, we have $e \wedge x = x$, so $\sim$ is a reflexive relation.

Suppose that $x = g \wedge y$ for $x, y \in X$ and $g \in G$. Then, by the solution to Exercise 3.2,

$$y = g^{-1} \wedge x,$$

which shows that $y \sim x$. Thus $\sim$ is symmetric.

If $x, y, z \in X$ are such that $x \sim y$ and $y \sim z$, we have

$$x = g \wedge y \quad \text{and} \quad y = h \wedge z$$

for some $g, h \in G$. Then

$$x = g \wedge (h \wedge z) = gh \wedge z$$

by the definition of group action. It follows that $x \sim z$, therefore $\sim$ is transitive. ■

The equivalence classes of the equivalence relation in Proposition 3.8 are precisely the orbits of the action of G on X. It follows that the orbits give a partition of X.

This fact is useful in proofs about finite groups acting on finite sets, because it tells us that the sum of the sizes of the orbits must be the total number of elements in the set: if

$$\mathrm{Orb}(x_1), \ldots, \mathrm{Orb}(x_n)$$

are the distinct orbits of X under the action of G, then

$$|X| = |\mathrm{Orb}(x_1)| + \cdots + |\mathrm{Orb}(x_n)|\,.$$

Now, the orbit of an element of X is a subset of the set X. The final idea that we want to look at in this chapter concerns certain subsets of the group G, rather than of the set X.

Definition 3.9 *Stabiliser*

If a group G acts on a set X and x is an element of X, then the **stabiliser** of x under G is the set

$$\mathrm{Stab}(x) = \{g : \ g \in G, \ g \wedge x = x\};$$

that is, the set of elements of G that fix x.

In Example 3.2,

$$\mathrm{Stab}(1) = \{e, s\},\ \mathrm{Stab}(2) = \left\{e, r^2 s\right\},\ \mathrm{Stab}(3) = D_3 \ \text{ and } \ \mathrm{Stab}(4) = \{e, rs\}.$$

In the action of D_6 on itself by conjugation, we can see that

$$\mathrm{Stab}(e) = \mathrm{Stab}(r^3) = D_6 \ \text{ and } \ \mathrm{Stab}(r) = \left\{e, r, r^2, r^3, r^4, r^5\right\}.$$

Exercise 3.7

Use Table 3.1 to determine the stabiliser of s under the action of D_6 on itself by conjugation.

You might have observed that all the stabilisers we have found so far are subgroups of the acting group. In the next exercise you are asked to prove that this is no coincidence.

Exercise 3.8

Show that, if G acts on X and $x \in X$, then $\mathrm{Stab}(x)$ is a subgroup of G.

We emphasise an important point about orbits and stabilisers.

If the group G acts on the set X, then:

- orbits are *subsets* of X
- stabilisers are *subgroups* of G.

Exercise 3.9

Suppose that S_3 acts on polynomials in three variables as described in Example 3.3. Write down the stabilisers of:

(a) $x_1x_2^2 + x_2x_3^2 + x_1^2x_3$

(b) $x_1x_2x_3$

(c) x_1x_2.

By now you are familiar with the action of D_6 on itself by conjugation, given by

$$g \wedge x = gxg^{-1}.$$

Any group, not just D_6, acts on itself in this way. The next exercise will show that this action of a group on itself is not the only one possible.

Exercise 3.10

Let $G = S_3$ and define an action of G on $X = S_3$ by

$$g \wedge x = gx.$$

(a) Show that $\wedge$ is a group action.

(b) Write down the orbits of this action.

(c) Write down the stabiliser of $(1\,2\,3)$.

We finish this subsection by stating and proving the Orbit–Stabiliser Theorem that, for a finite group, relates the size of the orbit to that of the stabiliser. First we derive a relationship between $\mathrm{Orb}(x)$ and the left cosets of the stabiliser of x.

Definition 3.10 *$Send_x(y)$*

Let G be a group acting on a set X and let $x \in X$. Then for each element y let

$$\mathrm{Send}_x(y) = \{g \in G : g \wedge x = y\}.$$

So $\mathrm{Send}_x(y)$ is the set of all elements of G that send x to y.

Exercise 3.11

Consider $D_3 = \{e, r, r^2, s, rs, r^2s\}$ and the action described in Example 3.2.

(a) Write down the left cosets of $\mathrm{Stab}(1) = \{e, s\}$.

(b) Write down $\mathrm{Send}_1(1), \mathrm{Send}_1(2)$ and $\mathrm{Send}_1(4)$.

It is no coincidence that the answers to the parts of Exercise 3.11 are the same (see also Example 5.1 of Chapter 5).

Lemma 3.11

Let G be a group acting on a set X, let $x \in X$ and $y \in \mathrm{Orb}(x)$. If $g \in G$ is such that $g \wedge x = y$, then

$$\mathrm{Send}_x(y) = g\mathrm{Stab}(x).$$

Proof Let $h \in \mathrm{Send}_x(y)$ and let $g \wedge x = y$. Then

$$(g^{-1}h) \wedge x = g^{-1} \wedge (h \wedge x) = g^{-1} \wedge y = x$$

by Exercise 3.2. So $g^{-1}h \in \mathrm{Stab}(x)$ and so, since $h = gg^{-1}h$, we have that $h \in g\mathrm{Stab}(x)$. Thus

$$\mathrm{Send}_x(y) \subseteq g\mathrm{Stab}(x).$$

Now suppose that $k \in g\mathrm{Stab}(x)$. Then $k = gh$ for some $h \in \mathrm{Stab}(x)$, and so

$$k \wedge x = (gh) \wedge x = g \wedge (h \wedge x) = g \wedge x = y$$

by definition of g and because $h \in \mathrm{Stab}(x)$. Thus $k \in \mathrm{Send}_x(y)$ and we have shown that

$$g\mathrm{Stab}(x) \subseteq \mathrm{Send}_x(y).$$

Hence $\mathrm{Send}_x(y) = g\mathrm{Stab}(x)$. ■

Lemma 3.11 implies that for each $x \in X$ we can define a function σ_x from $\mathrm{Orb}(x)$ to the set of cosets of $\mathrm{Stab}(x)$. The next theorem shows that this function is a bijection.

Theorem 3.12

Let G be a group acting on a set X, let $x \in X$ and let $H = \mathrm{Stab}(x)$. Let $C(x)$ be the set of left cosets of H in G. Then the function $\sigma_x : \mathrm{Orb}(x) \to C(x)$ defined by

$$\sigma_x : g \wedge x \mapsto gH$$

is a bijection.

Every element of $\mathrm{Orb}(x)$ can be written in the form $g \wedge x$ for some $g \in G$, by definition of $\mathrm{Orb}(x)$.

Proof We need to show that the function σ_x is well defined, one–one and onto.

Suppose that $g \wedge x = h \wedge x = y$. Then g and h both belong to $\mathrm{Send}_x(y)$. By Lemma 3.11, we have

$$\mathrm{Send}_x(y) = gH \quad \text{and} \quad \mathrm{Send}_x(y) = hH,$$

so $\sigma_x(g \wedge x) = gH = hH = \sigma_x(h \wedge x)$, meaning that σ_x is well defined.

To check that σ_x is one–one, pick $g \wedge x$ and $h \wedge x$ in $\mathrm{Orb}(x)$ such that $\sigma_x(g \wedge x) = \sigma_x(h \wedge x)$. Then

$$\begin{aligned} \sigma_x(g \wedge x) = \sigma_x(h \wedge x) &\Rightarrow gH = hH \\ &\Rightarrow h^{-1}g \in H \\ &\Rightarrow h^{-1}g \wedge x = x \quad \text{because } H = \mathrm{Stab}(x) \\ &\Rightarrow g \wedge x = h \wedge x, \end{aligned}$$

which shows that σ_x is one–one.

Finally, any coset gH of H is the image of the element $g \wedge x$ in $\mathrm{Orb}(x)$, which shows that σ_x is onto. ■

It is important to note that, while σ_x in Theorem 3.12 is a bijection, it is not an isomorphism, because the domain $\mathrm{Orb}(x)$ is not a group.

When G is a finite group, Lagrange's Theorem can be combined with Theorem 3.12 to obtain a relationship between the size of the orbit of an element and that of the stabiliser of the same element.

Corollary 3.13 *Orbit–Stabiliser Theorem*

Let G be a finite group acting on the set X. Then, for each $x \in X$,

$$|\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)| = |G|.$$

Proof By Theorem 3.12, the number of elements in $\mathrm{Orb}(x)$ is the same as the number m of left cosets of $\mathrm{Stab}(x)$.

Since the m cosets of $\mathrm{Stab}(x)$ partition G, we have

$$|G| = m\,|\mathrm{Stab}(x)| = |\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)|\,,$$

as required. ■

3.2 Cayley's Theorem

We have seen that several groups, for example the Klein group V, are isomorphic to a subgroup of the symmetric group S_4.

Recall that for any set X, the group of permutations on X (that is, the group of bijections from X to itself with composition of functions) is denoted by S_X. It is reasonable to ask which groups are isomorphic to a subgroup of S_X for some set X. The answer, perhaps surprisingly, is *all* groups.

This was first observed by the mathematician Arthur Cayley and we state this result as a theorem bearing his name.

We will prove Cayley's Theorem using an action of a group G on itself called the **action by left multiplication**. You met a special case of this action in Exercise 3.10. It is defined by

$$g \wedge x = gx \quad \text{for all} \quad g, x \in G.$$

We check that this definition gives indeed an action of G on itself using exactly the same method as in Exercise 3.10. First of all,

$$g \wedge x = gx \in X = G.$$

Moreover:

(a) $e \wedge x = ex = x$ for all $x \in X$

(b) $g \wedge (h \wedge x) = g \wedge (hx) = (gh)x = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

So, by Definition 3.1, G acts on itself by $\wedge$.

Before stating and proving Cayley's Theorem, we give an example that illustrates the method of proof.

Example 3.14 *An action by left multiplication*

Let $G = \{e, r, h, v\}$ be the group of symmetries of the rectangle and consider the action of G on itself by left multiplication. Number the elements of G as follows:

$$e = g_1, \quad r = g_2, \quad h = g_3 \quad \text{and} \quad v = g_4.$$

Now consider the action of r on each element of G:

$$r \wedge g_1 = rg_1 = g_2, \quad r \wedge g_2 = g_1, \quad r \wedge g_3 = g_4 \quad \text{and} \quad r \wedge g_4 = g_3.$$

Thus, the action of r swaps g_1 and g_2, and it also swaps g_3 and g_4. In fact, one way to describe this action is via a permutation f_r of G, namely

$$(g_1\, g_2)(g_3\, g_4).$$

Once we have numbered the elements of G, there is no ambiguity in denoting f_r via the indices of the elements it permutes, that is, via the permutation $(1\,2)(3\,4)$.

We can obtain a permutation representation for all the other elements of G in this way, and we get

$$f_e = e, \quad f_h = (1\,3)(2\,4) \quad \text{and} \quad f_v = (1\,4)(2\,3).$$

In fact, we can define a homomorphism $f : G \to S_4$ by

$$f : g \mapsto f_g.$$

This homomorphism is injective and the image

$$f(G) = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

is isomorphic to the Klein group.

Theorem 3.15 *Cayley's Theorem*

Every group G is isomorphic to a subgroup of S_G, the group of permutations of G.

In particular, if G is finite then G is isomorphic to a subgroup of S_n, where $n = |G|$.

Proof Let G act on itself by left multiplication, that is, by

$$g \wedge x = gx \text{ for all } g, x \in G.$$

Define a map $\phi : G \to S_G$, so that, for $g \in G$, $\phi(g) = \phi_g$ is the permutation of G given by

$$\phi_g(x) = g \wedge x = gx.$$

Then for g, h and x in G,

$$\phi_{gh}(x) = gh \wedge x = g \wedge (h \wedge x) = \phi_g \phi_h(x),$$

so ϕ is a homomorphism. This homomorphism is injective, for if $\phi_g = \phi_h$ then

$$g = ge = \phi_g(e) = \phi_h(e) = he = h.$$

Hence G is isomorphic to its image $\phi(G)$, which is a subgroup of S_G.

If G is finite and of order n then, as in Example 3.14, we identify S_G with S_n by numbering the elements of G from 1 to n. ■

Exercise 3.12

Use the approach given in the proof of Cayley's Theorem to find a subgroup of S_8 that is isomorphic to $G = \mathbb{Z}_4 \times \mathbb{Z}_2$.

Note that the homomorphism you found in Exercise 3.12 is by no means the only homomorphism between $\mathbb{Z}_4 \times \mathbb{Z}_2$ and a subgroup of a finite permutation group. Indeed, there may be simpler homomorphisms, and ones where the codomain is a subgroup of some S_n for $n \neq 8$. For example, we can construct a homomorphism from G to S_6 with

$(1, 0) \mapsto (1\,2\,3\,4)$ and
$(0, 1) \mapsto (5\,6)$.

3.3 Cauchy's Theorem

We now aim to prove that for any prime number p, every finite group G whose order is a multiple of p must contain an element of order p. This result is called Cauchy's Theorem. In order to prove Cauchy's Theorem, we work with a specific group action, and before we look at the general description of this action, we consider a particular example.

By now you should be quite familiar with the dihedral group

$$D_3 = \{e, r, r^2, s, rs, r^2 s\},$$

the group of symmetries of an equilateral triangle. The element r is the rotation about the centre of the triangle through $\frac{2\pi}{3}$, and s is the reflection shown in Figure 3.2. The elements rs and $r^2 s$ then give the other two reflections. Remember that

$$sr = r^2 s \quad \text{and} \quad sr^2 = rs.$$

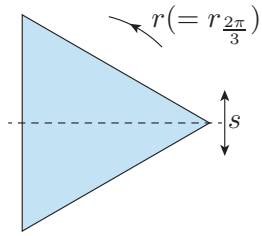

Figure 3.2 Symmetries of an equilateral triangle

There is an action of the group S_3 on the set Y of all triples (g_1, g_2, g_3) of elements of D_3 that works as follows. For $a \in S_3$, the action applies the permutation $a \in S_3$ to each component of the triple. For example,

$$(1\,2\,3) \wedge (r, r^2, e) = (e, r, r^2) \quad \text{and}$$
$$(1\,2) \wedge (r, r^2, e) = (r^2, r, e).$$

The requirements for an action are clearly satisfied – the second requirement follows from the fact that composition of functions is associative.

Now let $A = \langle (1\,2\,3) \rangle$ be the cyclic subgroup of S_3 generated by $(1\,2\,3)$ and let X be the set of triples (g_1, g_2, g_3), where each $g_i \in D_3$ and $g_1 g_2 g_3 = e$. Examples of elements of X are (r, r^2, e), (s, e, s) and, since r^2 has order 3, also (r^2, r^2, r^2). Notice that in each case we have $g_3 = (g_1 g_2)^{-1}$, which is equivalent to $g_1 g_2 g_3 = e$.

Now let $x = (g_1, g_2, g_3)$ be an element of X, so $g_1 g_2 g_3 = e$. The three elements of A act on x as follows:

$$e \wedge x = x, \quad (1\,2\,3) \wedge x = (g_3, g_1, g_2), \quad (1\,3\,2) \wedge x = (g_2, g_3, g_1).$$

We have

$$g_3 g_1 g_2 = (g_1 g_2)^{-1} g_1 g_2 = e \quad \text{and}$$
$$g_2 g_3 g_1 = g_2 (g_1 g_2)^{-1} g_1 = g_2 g_2^{-1} g_1^{-1} g_1 = e,$$

so $a \wedge x \in X$ for all $x \in X$ and all $a \in A$.

Thus we have indeed defined an action of the subgroup A on the set X.

How big is the set X? There are six independent choices for each of the first two elements g_1, g_2 of (g_1, g_2, g_3), since $|D_3| = 6$, but g_3 is then determined and must be $(g_1 g_2)^{-1}$. Therefore

$$|X| = 6 \times 6 = 36.$$

The next exercise is intended to help you understand the key points of the proof of Cauchy's Theorem, which follows it.

Exercise 3.13

Consider the action of A on X described above.

(a) Find $g_3 \in D_3$ such that $(r, s, g_3) \in X$. How many elements of X are in the orbit of (r, s, g_3)?

(b) Find $g_3 \in D_3$ such that $(r, r, g_3) \in X$. How many elements of X are in the orbit of (r, r, g_3)?

(c) Which elements (g_1, g_2, g_3) of X are stabilised by $(1\,2\,3)$?

Theorem 3.16 *Cauchy's Theorem*

Let G be a group of order n and let p be a prime divisor of n. Then G has an element of order p.

Proof Let A be the cyclic subgroup of S_p generated by $(1\,2\,\ldots\,p)$ and let X be the set of p-tuples $(g_1, g_2, \ldots, g_p)$ where each g_i is an element of G and

$$g_1 g_2 \cdots g_p = e.$$

Let $a \in A$ and let $x = (g_1, g_2, \ldots, g_p) \in X$. We check that $a \wedge x \in X$, where $\wedge$ is the action described above.

Now $g_p = (g_1 \cdots g_{p-1})^{-1}$, so $x = (g_1, \ldots, g_{p-1}, (g_1 g_2 \cdots g_{p-1})^{-1})$.

Then $a \wedge x$ is obtained from x by cyclically permuting the g_is, so

$$a \wedge x = (g_i, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}, g_1, \ldots, g_{i-1}) \text{ where } a(i) = 1.$$

Now

$$\begin{aligned} &g_i \cdots g_{p-1}(g_1 \cdots g_{p-1})^{-1} g_1 \cdots g_{i-1} \\ &\quad = (g_i \cdots g_{p-1} g_{p-1}^{-1} \cdots g_i^{-1})(g_{i-1}^{-1} \cdots g_1^{-1} g_1 \cdots g_{i-1}) \\ &\quad = e, \end{aligned}$$

and so $a \wedge x \in X$ as required. Hence A acts on X by $\wedge$.

Since A has prime order p, we know from Corollary 3.13 that each orbit of this action of A must have either p elements or 1 element. Let s be the number of orbits with p elements and t be the number of orbits with one element. The orbits partition X so X has precisely $ps + t$ elements.

We can count the number of elements in X in another way. For each of $g_1, g_2, \ldots, g_{p-1}$ we have n independent choices of elements of G, but then g_p is determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$.

Thus X has n^{p-1} elements. As p is a factor of n, we have that $n = pm$ for some integer m.

Hence $ps + t = |X| = n^{p-1} = (pm)^{p-1}$, and so

$$t = (pm)^{p-1} - ps = pq, \qquad \text{where } q = (p^{p-2}m^{p-1} - s).$$

Now $t > 0$, because the orbit of $(e, e, \ldots, e)$ has only one element. As $t = pq$ is a positive multiple of p it follows that $t \geq p > 1$.

We now know that, apart from $(e, e, \ldots, e)$, there is at least one other element $x = (g_1, g_2, \ldots, g_p)$ whose orbit has only one element. Such an element x is stabilised by $(1\,2\,\ldots\,p)$, so we must have $g_1 = g_2 = \cdots = g_p = g$, say, and $x = (g, g, \ldots, g)$. We have that $g^p = e$ because $x \in X$, and $g \neq e$ because $x \neq (e, e, \ldots, e)$.

By Exercise 4.7 of Chapter 5, the order of g must be a divisor of p. Since p is prime and g cannot have order 1, the order of g must be p. ■

Exercise 3.14

Let G be a group of order 6.

(a) Show that G has a cyclic subgroup of order 3 and a cyclic subgroup of order 2.

(b) Suppose that G is abelian. Let $a \in G$ have order 3 and $b \in G$ have order 2. What is the order of ab? Show that G is cyclic.

3.4 Finite abelian groups

We finish this chapter by proving some results that take us a further step along the way to classifying finite abelian groups.

Theorem 3.17

Let G be a finite abelian group of order n, where

$$n = p_1 p_2 \cdots p_r$$

for r distinct primes $p_1, p_2, \ldots, p_r$. Then G is cyclic and of order n. Moreover,

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r}.$$

Proof By Cauchy's Theorem, G has r cyclic subgroups $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_r}$.

For each i in $\{1, \ldots, r\}$, let g_i be a generator for $\mathbb{Z}_{p_i}$ so that g_i has order p_i. In fact, any non-identity element of $\mathbb{Z}_{p_i}$ generates the group.

Since $p_1, \ldots, p_r$ are distinct primes, the element $g_1 g_2 \cdots g_r$ has order

$$p_1 p_2 \cdots p_r = n$$

by the solution of Exercise 2.4. Thus G is cyclic and generated by this element.

It follows from Theorem 2.13 that $G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r}$, as required. ■

Theorem 3.17 applies to the rather special case of abelian groups whose order is a product of prime numbers. There is a result of the same flavour for abelian groups whose order is a *power* of a prime. This result requires a lemma whose proof is slightly technical and which uses additive notation for improved readability. The proof also makes use of Exercise 1.10.

In additive notation, Exercise 1.10 shows that if G is an abelian group and H_1, H_2 are subgroups of G with $H_1 \cap H_2 = \{0\}$, then whenever $h_1 \in H_1$ and $h_2 \in H_2$ are such that

$$h_1 + h_2 = 0,$$

then $h_1 = 0$ and $h_2 = 0$.

We pull out a small part of the proof of Lemma 3.18 below as an exercise.

Exercise 3.15

Suppose that G is an abelian group, written in additive notation, and let A be a subgroup of G. Suppose that $y \in G$, and $py, dy \in A$, where p and d are coprime integers. Show that $y \in A$.

Lemma 3.18

Suppose that G is an abelian group of order p^n for some prime p and some positive integer n. Then

$$G \cong H \times K,$$

where H is a cyclic subgroup of G of order p^r, for some positive integer r.

Proof By Proposition 4.5 of Chapter 5, the order of any element of G divides p^n. Choose $g \in G$ such that g has order p^r, where p^r is maximal among the orders of elements of G.

Let $H = \langle g \rangle$ be the cyclic subgroup generated by g. The maximality of p^r means that $p^r x = 0$ for all $x \in G$.

Consider the set of all subgroups of G whose intersection with H is $\{0\}$. This set is non-empty since it contains the trivial subgroup. Let K be maximal in this set. Then $H \cap K = \{0\}$, but for any proper subgroup K' of G such that $K \leq K'$ and $K' \neq K$ the maximality of K implies that $H \cap K' \neq \{0\}$.

K' is a *proper* subgroup of G if $K' \leq G$ and $K' \neq G$.

We aim to show that $G = H \times K$. By way of contradiction, let $x \in G \setminus (H \times K)$. Now

$$p^r x = 0 \in H \times K,$$

Recall that the notation $A \setminus B$, sometimes written $A - B$, denotes the set A excluding any elements of B.

so we can choose $m \leq r$ such that $p^m x \in H \times K$ but $p^{m-1}x \notin H \times K$ (if no such m existed, we would have $p^{m-1}x \in H \times K$ for all $m \in \{1, \ldots, r\}$, including $p^0 x = x$, contradicting our choice of x).

Let $y = p^{m-1}x$. Then, since $py \in H \times K$, we can write $py = ag + k$ for some $a \in \mathbb{Z}$ and $k \in K$.

From our choice of r, we have that

$$0 = p^r y = p^{r-1}(ag + k) = p^{r-1}ag + p^{r-1}k.$$

We started with an element y with $py \in H \times K$ but $y \notin H \times K$, and from this we have constructed an element $z = y - bg$ with $pz \in K$ but $z \notin K$.

Since $H \cap K = \{0\}$, by Exercise 1.10 this means that $p^{r-1}ag = 0$, and so p divides a. Thus we can write $py = pbg + k$ for some integer b, and so $p(y - bg) \in K$. Consider the element $y - bg$. Now, if $y - bg \in K$ then $y = bg + k_1$ for some $k_1 \in K$, which gives $y \in H \times K$. Since $y \notin H \times K$, we must have $y - bg \notin K$.

Let $K' = \langle K, y - bg \rangle$, the subgroup generated by K and $y - bg$. Then $K' \neq K$. By our choice of K, we have $K' \cap H \neq \{0\}$. Thus there exists $c \in \mathbb{Z}$ with $c \neq 0$ and

$$cg = k + d(y - bg).$$

Now p does not divide d, because $H \cap K = \{0\}$ and $p(y - bg) \in K$. Thus $\mathrm{hcf}(p, d) = 1$.

But now we have

$$dy = cg + dbg - k \in H \times K \quad \text{and} \quad py \in H \times K.$$

Thus, since $\mathrm{hcf}(p, d) = 1$, by Exercise 3.15 we have $y \in H \times K$, which is a contradiction.

This means that there can be no $x \in G \setminus H \times K$. So we have $G = H \times K$, as required. ■

Lemma 3.18 enables us to prove that every abelian group whose order is the power of a prime is a direct product of cyclic groups.

Theorem 3.19

Let G be an abelian group of order p^n for some positive integer n and for some prime p. Then G is a direct product of cyclic subgroups.

Proof We prove this result by induction on n.

Firstly, the result is true for $n = 1$, since in that case

$$G \cong \mathbb{Z}_p \, (\cong \mathbb{Z}_p \times \{0\}).$$

Now suppose that the result holds for all abelian groups of order p^m with $m < n$, and suppose that G has order p^n.

By Lemma 3.18, we know $G \cong H \times K$ where H is a non-trivial cyclic subgroup of G. Thus $|K|$ is p^m for some $m < n$, and we can use the induction hypothesis that K is a direct product of cyclic subgroups of K to conclude that G is a direct product of cyclic subgroups, as required. ■

Exercise 3.16

Let G be an abelian group of order 8. Write down all the possible groups to which G might be isomorphic.

We need just a little more machinery before we can prove that all finite abelian groups are direct products of cyclic groups. This result, which will be proved in Chapter 8, Subsection 2.1, will be one of the main results in this book.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Apply the Internal Direct Product Theorem in simple cases.

(b) Decide whether a given group is cyclic.

(c) Given a finite cyclic group, find a generator for a subgroup of a given order.

(d) Express a given finite cyclic group as the direct product of cyclic groups of prime power order.

(e) Given two direct products of cyclic groups, determine whether or not they are isomorphic.

(f) For a group G and a set X, check whether a given function $G \times X \to X$ is a group action.

(g) Identify the orbit of an element of a set X acted on by a group G.

(h) Identify the stabiliser of an element of a set X acted on by a group G.

(i) Apply Cauchy's Theorem to show the existence of certain subgroups of prime order.

(j) Work with the action used in the proof of Cauchy's Theorem in specific examples of groups.

(k) Prove simple results about abelian groups, cyclic groups and direct products.

Solutions to exercises

Solution to Exercise 1.1

Closure Let (x_1, y_1) and (x_2, y_2) be any two elements of $\mathbb{R} \times \mathbb{R}$. By definition, x_1, y_1, x_2 and y_2 are in $\mathbb{R}$. Since $\mathbb{R}$ is closed under addition, it follows that $x_1 + x_2$ and $y_1 + y_2$ are also in $\mathbb{R}$. By definition,

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

so, by the above, this sum is an element of $\mathbb{R} \times \mathbb{R}$. Therefore the operation $+$ satisfies the closure axiom.

Associativity Let (x_1, y_1), (x_2, y_2) and (x_3, y_3) be three elements of $\mathbb{R} \times \mathbb{R}$. By definition,

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \text{ and}$$
$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1 + (x_2 + x_3),\ y_1 + (y_2 + y_3)).$$

The right-hand sides of these two equations are equal, since addition in $\mathbb{R}$ is associative. Hence

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1, y_1) + ((x_2, y_2) + (x_3, y_3))$$

and so $+$ in $\mathbb{R} \times \mathbb{R}$ is associative.

Identity The element $(0, 0)$ belongs to $\mathbb{R} \times \mathbb{R}$, and

$$(0, 0) + (x, y) = (x, y) + (0, 0) = (x, y)$$

for any (x, y) in $\mathbb{R} \times \mathbb{R}$. Therefore $(0, 0)$ is the identity of $\mathbb{R} \times \mathbb{R}$, and the identity axiom is satisfied.

Inverses If (x, y) is any element of $\mathbb{R} \times \mathbb{R}$ then, as x and y are in $\mathbb{R}$, their additive inverses $-x$ and $-y$ are also in $\mathbb{R}$. So the element $(-x, -y)$ is an element of $\mathbb{R} \times \mathbb{R}$. Furthermore,

$$(x, y) + (-x, -y) = (0, 0) = (-x, -y) + (x, y).$$

So $(-x, -y)$ is the inverse of the element (x, y), and the inverses axiom is satisfied.

Solution to Exercise 1.2

The underlying set is

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_3 &= \{0, 1\} \times \{0, 1, 2\} \\ &= \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}. \end{aligned}$$

The Cayley table is constructed using addition modulo 2 for the first components and addition modulo 3 for the second.

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Solution to Exercise 1.3

(a) Let (g_1, h_1), (g_2, h_2) and (g_3, h_3) be any three elements of $G \times H$. Then

$$\begin{aligned}
&((g_1, h_1) \bullet (g_2, h_2)) \bullet (g_3, h_3) \\
&\quad = (g_1 \circ g_2, h_1 * h_2) \bullet (g_3, h_3) && \text{by the definition of } \bullet \\
&\quad = ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) && \text{by the definition of } \bullet \\
&\quad = (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) && \text{by the associativity axiom for } G \text{ and } H \\
&\quad = (g_1, h_1) \bullet ((g_2 \circ g_3), (h_2 * h_3)) && \text{by the definition of } \bullet \\
&\quad = (g_1, h_1) \bullet ((g_2, h_2) \bullet (g_3, h_3)) && \text{by the definition of } \bullet .
\end{aligned}$$

(b) Let (g, h) be any element of the direct product $G \times H$. Then

$$\begin{aligned}
(e_G, e_H) \bullet (g, h) &= (e_G \circ g, e_H * h) && \text{by the definition of } \bullet \\
&= (g, h) && \text{by the identity axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g, h) \bullet (e_G, e_H) = (g, h).$$

Hence (e_G, e_H) is the identity element of the direct product.

(c) Applying the inverse properties for the groups G and H, we have

$$\begin{aligned}
(g, h) \bullet (g^{-1}, h^{-1}) &= (g \circ g^{-1}, h * h^{-1}) && \text{by the definition of } \bullet \\
&= (e_G, e_H) && \text{by the inverses axiom for } G \text{ and } H.
\end{aligned}$$

Similarly,

$$(g^{-1}, h^{-1}) \bullet (g, h) = (e_G, e_H).$$

Hence (g^{-1}, h^{-1}) is the inverse of (g, h).

Solution to Exercise 1.4

Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then

$$\begin{aligned}
(g_1, h_1)(g_2, h_2) &= (g_1 g_2, h_1 h_2) \\
&= (g_2 g_1, h_2 h_1)
\end{aligned}$$

since G and H are both abelian. But

$$(g_2 g_1, h_2 h_1) = (g_2, h_2)(g_1, h_1),$$

so the direct product $G \times H$ is abelian.

Solution to Exercise 1.5

Assume that $h \in H_1 \cap H_2$. We can express h in two ways as an element of H_1H_2, namely

$$h = he, \text{ with } h \in H_1,\ e \in H_2, \text{ and}$$
$$h = eh, \text{ with } e \in H_1,\ h \in H_2.$$

Hence $\phi(h, e) = \phi(e, h)$, and, since ϕ is one–one, we have

$$(h, e) = (e, h).$$

Then $h = e$ by the definition of an ordered pair. Thus the only element in $H_1 \cap H_2$ is the identity, as required.

Solution to Exercise 1.6

As before, we write $a = h_1h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.

Let aha^{-1} be any element of aH_2a^{-1}, where $h \in H_2$. Then

$$\begin{aligned} aha^{-1} &= (h_1h_2)h(h_1h_2)^{-1} \\ &= h_1h_2hh_2^{-1}h_1^{-1} \\ &= h_1(h_2hh_2^{-1})h_1^{-1} \\ &= h_1h'h_1^{-1} \qquad (\text{where } h' = h_2hh_2^{-1} \in H_2) \\ &= h'h_1h_1^{-1} \qquad (\text{since } h_1 \in H_1 \text{ and } h' \in H_2 \text{ commute}) \\ &= h' \in H_2, \end{aligned}$$

and so $aH_2a^{-1} \subseteq H_2$.

Solution to Exercise 1.7

We can define the subgroups as follows:

$$H_1 = \langle a^3 \rangle = \{e, a^3\},$$
$$H_2 = \langle a^2 \rangle = \{e, a^2, a^4\}.$$

Note that $H_1 \cong \mathbb{Z}_2$ and $H_2 \cong \mathbb{Z}_3$.

Since e, a^2, a^3, a^4, a^5 are all in H_1H_2 and

$$a^3a^4 = a^7 = a,$$

we see that $\mathbb{Z}_6 = H_1H_2$.

Next, by inspection, $H_1 \cap H_2 = \{e\}$.

Lastly, we must check that H_1 and H_2 are both normal in $\mathbb{Z}_6$. But $\mathbb{Z}_6$ is abelian, so every subgroup is normal.

Hence H_1 and H_2 satisfy the conditions in Theorem 1.5, and we can conclude that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, as required.

Solution to Exercise 1.8

Let $g = h^{-1}k^{-1}hk$. Since K is a normal subgroup of $G, h^{-1}k^{-1}h \in K$; and so, since $k \in K, g \in K$. Since H is a normal subgroup of G, $k^{-1}hk \in H$; and so, since $h \in H, g \in H$. Thus $g \in H \cap K = \{e\}$ and so $g = e$. That is, $h^{-1}k^{-1}hk = e$, and so by multiplying on the left by kh we see that $hk = kh$.

Solution to Exercise 1.9

Suppose that $\psi(a_1, (b_1, c_1)) = \psi(a_2, (b_2, c_2))$. By the definition of ψ,

$$((a_1, b_1), c_1) = ((a_2, b_2), c_2).$$

By the definition of ordered pairs, $(a_1, b_1) = (a_2, b_2)$ and $c_1 = c_2$. Applying the definition of ordered pairs again, we get $a_1 = a_2$ and $b_1 = b_2$. Hence $(a_1, (b_1, c_1)) = (a_2, (b_2, c_2))$. This shows that ψ is one–one.

To see that ψ is onto, let $((a, b), c)$ be any element of the codomain. Then $a \in A, b \in B, c \in C$, and so $(a, (b, c)) \in A \times (B \times C)$ and $\psi(a, (b, c)) = ((a, b), c)$. Hence ψ is onto.

To check the morphism property, let $(a_1, (b_1, c_1))$ and $(a_2, (b_2, c_2))$ be any two elements of the domain. Then

$$\begin{aligned}
\psi((a_1, (b_1, c_1))(a_2, (b_2, c_2))) &= \psi(a_1a_2, ((b_1, c_1)(b_2, c_2))) \\
&= \psi(a_1a_2, (b_1b_2, c_1c_2)) \\
&= ((a_1a_2, b_1b_2), c_1c_2) \\
&= ((a_1, b_1)(a_2, b_2), c_1c_2) \\
&= ((a_1, b_1), c_1)((a_2, b_2), c_2) \\
&= \psi(a_1, (b_1, c_1))\psi((a_2, (b_2, c_2)).
\end{aligned}$$

This completes the proof that ψ is an isomorphism.

Solution to Exercise 1.10

Since G is abelian, the elements of H_1 and H_2 commute, so we can apply Proposition 1.9(b) to conclude that $H_1H_2 \cong H_1 \times H_2$ via the isomorphism $\psi : H_1H_2 \to H_1 \times H_2$ defined by

$$x_1x_2 \mapsto (x_1, x_2).$$

If $h_1h_2 = 1$, then $(h_1, h_2) = \psi(h_1h_2) = \psi(1)$. Since ψ must map the identity in H_1H_2 to the identity in $H_1 \times H_2$, we must have $(h_1, h_2) = (1, 1)$, which gives the required result.

Solution to Exercise 2.1

(a) Since m is the least positive exponent such that a^m is in H, we have $k \geq m$ and we can use the Division Algorithm (Book A, Chapter 1, Theorem 4.1) to write $k = mq + r$ where $0 \leq r < m$. Hence $r = k - mq$, and so

$$\begin{aligned}
a^r &= a^{k-mq} \\
&= a^k a^{-mq} \\
&= a^k (a^m)^{-q}.
\end{aligned}$$

Since a^k and a^m belong to H, so does a^r.

Now, m was chosen as the least *positive* exponent appearing in H, so we must have $r = 0$, and hence $m \mid k$. We have shown that every element a^k of H is a power $a^k = a^{mq} = (a^m)^q$ of a^m, which completes the proof that $H = \langle a^m \rangle$.

(b) Since $a^n = e$, which is an element of H, from part (a) we have that $m \mid n$.

(c) Let $n = mq$. We first observe that $e = a^n = a^{mq} = (a^m)^q$. So q is a positive power of a^m that produces the identity. It remains to prove that q is the smallest such power of a^m.

Consider a positive power k of a^m that is the identity; that is, $e = (a^m)^k = a^{mk}$. Since the order of a is n, this can only be true if $mk \geq n = mq$. Hence $k \geq q$. Therefore q is the least power of a^m that gives the identity. Hence the order of a^m, and therefore the order of H, is q.

Solution to Exercise 2.2

(a) The divisors of 24 are $1, 2, 3, 4, 6, 8, 12$ and 24, so $\mathbb{Z}_{24}$ will have a subgroup of each of these orders.

(b) (i) The subgroups are isomorphic to $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ and $\mathbb{Z}_{24}$, respectively.

(ii) The first subgroup in the list is the trivial subgroup, generated by $\frac{24}{1} \equiv 0 \pmod{24}$.

The remaining ones have generators $12, 8, 6, 4, 3, 2$ and 1, respectively.

We list the generators, the elements generated and the cyclic group to which the subgroup is isomorphic in the table below.

Generator (mod 24)	Elements generated	Isomorphic group
$\frac{24}{1} \equiv 0$	$\{0\}$	$\mathbb{Z}_1$
$\frac{24}{2} \equiv 12$	$\{0, 12\}$	$\mathbb{Z}_2$
$\frac{24}{3} \equiv 8$	$\{0, 8, 16\}$	$\mathbb{Z}_3$
$\frac{24}{4} \equiv 6$	$\{0, 6, 12, 18\}$	$\mathbb{Z}_4$
$\frac{24}{6} \equiv 4$	$\{0, 4, 8, 12, 16, 20\}$	$\mathbb{Z}_6$
$\frac{24}{8} \equiv 3$	$\{0, 3, 6, 9, 12, 15, 18, 21\}$	$\mathbb{Z}_8$
$\frac{24}{12} \equiv 2$	$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$	$\mathbb{Z}_{12}$
$\frac{24}{24} \equiv 1$	$\{0, 1, \ldots, 23\}$	$\mathbb{Z}_{24}$

Solution to Exercise 2.3

We use additive notation so that $(0,0)$ denotes the identity in both cases, and we write $n(x,y)$ for $\underbrace{(x,y)+\cdots+(x,y)}_{n \text{ times}}$.

(a) We have $(1,1) = (1,1)$, $2(1,1) = (0,2)$, $3(1,1) = (1,0)$,
$4(1,1) = (0,1)$, $5(1,1) = (1,2)$, $6(1,1) = (0,0)$.
Hence $(1,1)$ has order 6.

(b) We have $1(1,1) = (1,1)$ and $2(1,1) = (0,0)$. Hence $(1,1)$ has order 2.

Solution to Exercise 2.4

We use induction on r, the number of elements in the product. For $r = 2$, the result follows from Lemma 2.7, since G is abelian and p_1 and p_2 are distinct primes, so that $\langle g_1\rangle \cap \langle g_2\rangle = \{e\}$.

Suppose the result is true for $r = k$; that is, if $g_1, g_2, \ldots, g_k$ are elements of G that have distinct prime order $p_1, p_2, \ldots, p_r$ respectively, then the order of $g_1 g_2 \cdots g_k$ is $p_1 p_2 \cdots p_k$.

Let g_{k+1} be an element of G of order p_{k+1}, where p_{k+1} is prime and distinct from $p_1, p_2, \ldots, p_k$. Then

$$\langle g_1 g_2 \cdots g_k\rangle \cap \langle g_{k+1}\rangle = \{e\}$$

since no elements of $\langle g_1 g_2 \cdots g_k\rangle$ can have order p_{k+1}, and so we can apply Lemma 2.7 to obtain that the order of $g_1 g_2 \cdots g_{k+1}$ is $p_1 p_2 \cdots p_{k+1}$.

The result follows by induction.

Solution to Exercise 2.5

By Proposition 2.8, the order of the element $(1,1)$ in the direct product is the least common multiple of the orders of the element 1 in each of the factor groups.

(a) The order of 1 in $\mathbb{Z}_3$ is 3 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(3,5) = 15$, the element $(1,1)$ has order 15 in $\mathbb{Z}_3 \times \mathbb{Z}_5$.
As $\mathbb{Z}_3 \times \mathbb{Z}_5$ has 15 elements, it is cyclic.

(b) The order of 1 in $\mathbb{Z}_4$ is 4 and the order of 1 in $\mathbb{Z}_5$ is 5.
Since $\operatorname{lcm}(4,5) = 20$, the element $(1,1)$ has order 20 in $\mathbb{Z}_4 \times \mathbb{Z}_5$.
As $\mathbb{Z}_4 \times \mathbb{Z}_5$ has 20 elements, it is cyclic.

Solution to Exercise 2.6

(a) The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_4$ is 4.
Since $\operatorname{lcm}(2,4) = 4$, the element $(1,1)$ has order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_4$.
As $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 8 elements, it is not generated by $(1,1)$.

All we have done is to show that $(1,1)$ is not a generator. To show that the direct product is not cyclic, we would have to show that *none* of the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ generates the whole group.

(b) If (a, b) is any element of $\mathbb{Z}_2 \times \mathbb{Z}_4$, then a has order 1 or 2 and b has order 1, 2 or 4. The only possible least common multiples of the orders of a and b are 1, 2 and 4. Hence no element of the direct product has order 8, and so $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

Solution to Exercise 2.7

Let $a \in \mathbb{Z}_6$. Then $6a = 0$. Similarly, if $b \in \mathbb{Z}_8$, then $8b = 0$. Hence for any element (a, b) in $\mathbb{Z}_6 \times \mathbb{Z}_8$, we have

$$\begin{aligned} 24(a, b) &= (24a, 24b) \\ &= (4(6a), 3(8b)) \\ &= (0, 0). \end{aligned}$$

So the maximum order of any element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ is at most 24. Since this direct product has order 48, it cannot be cyclic.

Solution to Exercise 2.8

(a) The maximum order of an element of S_3 is 3.

(b) The maximum order of an element of $\mathbb{Z}_3$ is 3.

(c) The lowest common multiple is 3.

(d) $((1\,2), 1)$ has order 6.

Solution to Exercise 2.9

(a) The group $\mathbb{Z}_4 \times \mathbb{Z}_6$ is not cyclic.

The maximum order of an element in $\mathbb{Z}_4$ is 4 and the maximum order for an element of $\mathbb{Z}_6$ is 6. Since $\operatorname{lcm}(4, 6) = 12$, the maximum order for any element is at most 12.

Therefore the direct product, of order 24, is not cyclic.

(b) The group $\mathbb{Z}_2 \times \mathbb{Z}_9$ is cyclic.

Previous examples suggest that $(1, 1)$ should be a generator, which we can confirm as follows.

The order of 1 in $\mathbb{Z}_2$ is 2 and the order of 1 in $\mathbb{Z}_9$ is 9. Since $\operatorname{lcm}(2, 9) = 18$, the element $(1, 1)$ has order 18 in the direct product. As the direct product has 18 elements, it is cyclic.

Solution to Exercise 2.10

By Proposition 2.10, no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ can have order greater than the least common multiple of m and n.

Since m and n are not coprime, we have that $\operatorname{lcm}(m, n) < mn$, the order of the direct product. Hence no element can generate the whole of the direct product, and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Solution to Exercise 2.11

We have $90 = 2 \times 45$. Since 2 and 45 are coprime, we can deduce from Corollary 2.12 that

$$\mathbb{Z}_{90} \cong \mathbb{Z}_2 \times \mathbb{Z}_{45}.$$

Similarly, since $45 = 9 \times 5$ and these factors are coprime, we have

$$\mathbb{Z}_{45} \cong \mathbb{Z}_9 \times \mathbb{Z}_5.$$

Combining these results gives

$$\begin{aligned} \mathbb{Z}_{90} &\cong \mathbb{Z}_2 \times \mathbb{Z}_{45} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5. \end{aligned}$$

Solution to Exercise 2.12

We use induction on r, the number of distinct prime factors, and generalise the argument used in the solution to Exercise 2.11.

Firstly, if $r = 1$ the result is immediate. Now suppose that the result is true for $r - 1$ and write

$$\begin{aligned} n &= p_1^{k_1} (p_2^{k_2} \cdots p_r^{k_r}) \\ &= n_1(n_2 \cdots n_r), \end{aligned}$$

where, because all the p_i are distinct, the factors n_1 and $n_2 \cdots n_r$ are coprime. By Corollary 2.12, we have

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2 \cdots n_r}.$$

But $\mathbb{Z}_{n_2 \cdots n_r} \cong \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ by the inductive hypothesis, hence the result holds for $\mathbb{Z}_n$ by Proposition 1.10.

Solution to Exercise 2.13

We apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$. For example, since $154 = 2 \times 7 \times 11$, we have

$$\mathbb{Z}_{154} \cong \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}.$$

Hence
$$\begin{aligned} \mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5 &\cong (\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_5) \times \mathbb{Z}_5 \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$$

Note that 4 is a prime power and it cannot be factorised into distinct primes.

Similarly, we apply Theorem 2.13 to each of the cyclic factors appearing in the direct product $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$. This gives

$$\begin{aligned} \mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10} &\cong (\mathbb{Z}_5 \times \mathbb{Z}_{11}) \times (\mathbb{Z}_4 \times \mathbb{Z}_7) \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_5 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \times \mathbb{Z}_{11}. \end{aligned}$$

Thus the two groups $\mathbb{Z}_{154} \times \mathbb{Z}_{20} \times \mathbb{Z}_5$ and $\mathbb{Z}_{55} \times \mathbb{Z}_{28} \times \mathbb{Z}_{10}$ are isomorphic to the same direct product and hence to one another.

Solution to Exercise 2.14

(a) $$\begin{aligned}\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{75} &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_{25}) \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{25} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{5^2}.\end{aligned}$$

(b) $$\begin{aligned}\mathbb{Z}_9 \times \mathbb{Z}_{21} \times \mathbb{Z}_{245} &\cong \mathbb{Z}_9 \times (\mathbb{Z}_3 \times \mathbb{Z}_7) \times (\mathbb{Z}_5 \times \mathbb{Z}_{49}) \\ &\cong (\mathbb{Z}_3 \times \mathbb{Z}_9) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{49}) \\ &= (\mathbb{Z}_3 \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_{7^2}).\end{aligned}$$

Solution to Exercise 3.1

In each case we use commutativity of addition and multiplication in P_4 to write the variables in the polynomials in a 'natural' order.

(a) $(1\,2)(3\,4) \wedge x_1x_2x_3 - x_4 = x_1x_2x_4 - x_3$

(b) $(1\,2)(3\,4) \wedge x_1x_2 - x_3x_4 = x_1x_2 - x_3x_4$

(c) $(1\,2\,3\,4) \wedge x_1 + x_2 + x_3 + x_4 = x_1 + x_2 + x_3 + x_4$

Solution to Exercise 3.2

By Definition 3.1,

$$g^{-1} \wedge y = g^{-1} \wedge (g \wedge x) = (g^{-1}g) \wedge x = e \wedge x = x.$$

Solution to Exercise 3.3

(a) Pre- and post-multiplying the equation $sr = r^{-1}s$ by r and r^{-1} respectively gives

$$\begin{aligned}sr = r^{-1}s &\Rightarrow rsr = rr^{-1}s \\ &\Rightarrow rsrr^{-1} = rr^{-1}sr^{-1} \\ &\Rightarrow rs = sr^{-1}, \quad \text{as required.}\end{aligned}$$

(b) $$\begin{aligned}rs = sr^{-1} &\Rightarrow srs = ssr^{-1} = r^{-1} \quad \text{and} \\ rs = sr^{-1} &\Rightarrow rss = sr^{-1}s \\ &\Rightarrow r = sr^{-1}s.\end{aligned}$$

(c) Recall that $s = s^{-1}$. Using the formula for the power of a conjugate preceding the exercise, and part (b), gives

$$sr^ms = (srs)^m = r^{-m}.$$

Similarly,

$$sr^{-m}s = (sr^{-1}s)^m = r^m.$$

(d) Pre-multiplying both sides of the first equation by s gives

$$sr^ms = r^{-m} \Rightarrow r^ms = sr^{-m}.$$

Post-multiplying both sides of the second equation by s gives

$$sr^{-m}s = r^m \Rightarrow r^{-m}s = sr^m.$$

Solution to Exercise 3.4

We will use the equality $s = s^{-1}$ repeatedly.

(a) $r^m \wedge r^n = r^m r^n r^{-m} = r^n$

(b)
$$\begin{aligned} r^m \wedge r^n s &= r^m (r^n s) r^{-m} \\ &= r^{m+n} s r^{-m} \\ &= r^{m+n} r^m s \text{ using } s r^{-m} = r^m s \quad \text{(from Exercise 3.3)} \\ &= r^{2m+n} s \end{aligned}$$

(c)
$$\begin{aligned} r^m s \wedge r^n &= r^m s (r^n)(r^m s)^{-1} \\ &= r^m s (r^n) s r^{-m} \\ &= r^m (s r^n s) r^{-m} \\ &= r^m r^{-n} r^{-m} \text{ using } s r^n s = r^{-n} \quad \text{(from Exercise 3.3 with } m = n\text{)} \\ &= r^{-n} \end{aligned}$$

(d)
$$\begin{aligned} r^m s \wedge r^n s &= r^m s (r^n s)(r^m s)^{-1} \\ &= r^m s (r^n s) s r^{-m} \\ &= r^m s r^n (ss) r^{-m} \\ &= r^m s r^{n-m} \quad \text{(since } ss = e\text{)} \\ &= r^m r^{m-n} s \text{ using } s r^m = r^{-m} s \quad \text{(from Exercise 3.3)} \\ &= r^{2m-n} s \end{aligned}$$

Solution to Exercise 3.5

We read the orbits from the columns of Table 3.1.

$$\begin{array}{ll} \mathrm{Orb}(e) = \{e\} & \mathrm{Orb}(s) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}(r) = \{r,\ r^5\} & \mathrm{Orb}\left(r^2 s\right) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}\left(r^5\right) = \{r,\ r^5\} & \mathrm{Orb}\left(r^4 s\right) = \{s,\ r^2 s,\ r^4 s\} \\ \mathrm{Orb}\left(r^2\right) = \{r^2,\ r^4\} & \mathrm{Orb}(rs) = \{rs,\ r^3 s,\ r^5 s\} \\ \mathrm{Orb}\left(r^4\right) = \{r^2,\ r^4\} & \mathrm{Orb}\left(r^3 s\right) = \{rs,\ r^3 s,\ r^5 s\} \\ \mathrm{Orb}\left(r^3\right) = \{r^3\} & \mathrm{Orb}\left(r^5 s\right) = \{rs,\ r^3 s,\ r^5 s\} \end{array}$$

Solution to Exercise 3.6

(a) $\mathrm{Orb}(x_1x_2x_3 - x_4) =$
$\{x_1x_2x_3 - x_4, x_2x_3x_4 - x_1, x_1x_3x_4 - x_2, x_1x_2x_4 - x_3\}$

(b) $\mathrm{Orb}(x_1x_2x_3x_4) = \{x_1x_2x_3x_4\}$

(c) $\mathrm{Orb}(x_1x_2 + x_3x_4) = \{x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$

Solution to Exercise 3.7

In the column of Table 3.1 headed by s, the element s occurs 4 times. The stabiliser is

$$\mathrm{Stab}(s) = \left\{e,\ r^3,\ s,\ r^3 s\right\}.$$

Solution to Exercise 3.8

Closure Suppose that g and h are in $\mathrm{Stab}(x)$. Then

$$\begin{aligned}(gh) \wedge x &= g \wedge (h \wedge x) && \text{(by the definition of group action)}\\ &= g \wedge x && \text{(since } h \text{ fixes } x)\\ &= x && \text{(since } g \text{ fixes } x).\end{aligned}$$

Hence gh is in $\mathrm{Stab}(x)$ and $\mathrm{Stab}(x)$ is closed.

Identity By the definition of a group action, we know that $e \wedge x = x$ for any $x \in X$. This shows that e is in $\mathrm{Stab}(x)$.

Inverses Suppose $g \in \mathrm{Stab}(x)$. Then $x = g \wedge x$ and so

$$\begin{aligned}g^{-1} \wedge x &= g^{-1} \wedge (g \wedge x)\\ &= \left(g^{-1}g\right) \wedge x && \text{(by the definition of group action)}\\ &= e \wedge x\\ &= x.\end{aligned}$$

Hence $g^{-1} \in \mathrm{Stab}(x)$.

This completes the proof that $\mathrm{Stab}(x)$ is a subgroup of G.

Solution to Exercise 3.9

(a) $\mathrm{Stab}(x_1x_2^2 + x_2x_3^2 + x_1^2x_3) = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

(b) $\mathrm{Stab}(x_1x_2x_3) = S_3$

(c) $\mathrm{Stab}(x_1x_2) = \{e, (1\ 2)\}$

Solution to Exercise 3.10

(a) We can see that $g \wedge x = gx \in X = S_3$.

We check properties (a) and (b) of Definition 3.1.

(a) $e \wedge x = ex = x$ for all $x \in X$.

(b) $g \wedge (h \wedge x) = g \wedge (hx) = (gh)x = (gh) \wedge x$ for all $g, h \in G$ and all $x \in X$.

(b) $\mathrm{Orb}(e) = S_3$, so there is just one orbit.

(c) $\mathrm{Stab}((1\,2\,3)) = \{e\}$.

Solution to Exercise 3.11

(a) $\{e, s\}, \{r, rs\}, \left\{r^2, r^2s\right\}$

(b) $\mathrm{Send}_1(1) = \{e, s\}, \quad \mathrm{Send}_1(2) = \{r, rs\}, \quad \mathrm{Send}_1(4) = \left\{r^2, r^2s\right\}.$

Solution to Exercise 3.12

First we assign a number to each element of G.

$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8

Now we find the permutations given by the group action $g \wedge x = gx$.

For example, $g_3 = (2,0)$ generates the following permutation of $\mathbb{Z}_4 \times \mathbb{Z}_2$ (written using two-line notation for $\mathbb{Z}_4 \times \mathbb{Z}_2$).

$$\begin{pmatrix} (0,0) & (1,0) & (2,0) & (3,0) & (0,1) & (1,1) & (2,1) & (3,1) \\ (2,0) & (3,0) & (0,0) & (1,0) & (2,1) & (3,1) & (0,1) & (1,1) \end{pmatrix}$$

This can be written as

$$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_3 & g_4 & g_1 & g_2 & g_7 & g_8 & g_5 & g_6 \end{pmatrix},$$

or, in two-line notation for S_8 (we just remove the gs) as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix},$$

giving the permutation $(1\,3)(2\,4)(5\,7)(6\,8)$ in cycle notation.

The complete list of permutations in S_8 induced by an element of $\mathbb{Z}_4 \times \mathbb{Z}_2$ is as follows.

$(0,0) \mapsto e$
$(1,0) \mapsto (1\,2\,3\,4)(5\,6\,7\,8)$
$(2,0) \mapsto (1\,3)(2\,4)(5\,7)(6\,8)$
$(3,0) \mapsto (1\,4\,3\,2)(5\,8\,7\,6)$
$(0,1) \mapsto (1\,5)(2\,6)(3\,7)(4\,8)$
$(1,1) \mapsto (1\,6\,3\,8)(2\,7\,4\,5)$
$(2,1) \mapsto (1\,7)(2\,8)(3\,5)(4\,6)$
$(3,1) \mapsto (1\,8\,3\,6)(2\,5\,4\,7)$

This list defines a mapping that gives a homomorphism from G to a subgroup of S_8.

Solution to Exercise 3.13

(a) $g_3 = (rs)^{-1} = sr^{-1} = sr^2 = rs$. Since there are three distinct elements in the tuple, the orbit will have three elements (one for each possible permutation of the three elements).

(b) $g_3 = (r^2)^{-1} = r$. There is only one element in this orbit.

(c) The elements $(r,r,r), (e,e,e), (r^2,r^2,r^2)$ are stabilised by $(1\,2\,3)$. There can be no others, since any triple stabilised by $(1\,2\,3)$ has the form (a,a,a), so $a^3 = e$.

Solution to Exercise 3.14

(a) Since 2 and 3 are both prime and divide 6, by Cauchy's Theorem the group G has an element g of order 2 and an element h of order 3. Then the subgroups $\langle g \rangle$ and $\langle h \rangle$ are cyclic and of order 2 and 3 respectively.

(b) The product ab has order 6, and so $G = \langle ab \rangle$ is cyclic.

Solution to Exercise 3.15

Since p and d are coprime integers, there exist integers s and t such that $sp + td = 1$. Then

$$y = (sp + dt)y = s(py) + t(dy) \in A.$$

Solution to Exercise 3.16

Since $8 = 2^3$, we know from Theorem 3.19 that G is a direct product of cyclic groups. The possibilities are:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

We have not included $\mathbb{Z}_2 \times \mathbb{Z}_4$, because this group is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.